Orange
Cyberdefense

Security Navigator

Research-driven insights to build a safer digital society

Hugues Foulon
Executive Director
of Strategy and
Cybersecurity activities
Orange Cyberdefense

Michel Van Den Berghe
Chief Executive Officer
Orange Cyberdefense

Im Jahr 2019 analysierten wir über unsere 16 CyberSOCs/SOCs täglich mehr als 50 Milliarden Ereignisse, lösten über 35.000 Sicherheitsvorfälle und führten mehr als 170 Einsätze zur Bewältigung von Vorfällen durch. Unsere Experten haben all diese einzigartigen Informationen ausgewertet und die wichtigsten Ergebnisse in diesem Bericht zusammengefasst, zum Nutzen unserer Kunden und der gesamten Cybersecurity Community

Wir freuen uns, Ihnen die erste Ausgabe des Orange Cyberdefense Security Navigator zu präsentieren.

Dank unserer Position als einer der größten Telekommunikationsbetreiber der Welt (Orange) und als europäischer Marktführer für Cybersicherheit (Orange Cyberdefense) haben wir eine besondere Sicht auf die Bedrohungslage.

Die COVID-19-Pandemie hat die physische und digitale Gesellschaft wie die Wirtschaft in einem noch nie dagewesenen Ausmaß erschüttert. Sie hat die Art und Weise, wie wir arbeiten und Geschäfte machen, fundamental verändert. Viele dieser Veränderungen werden die Krise überdauern. Die Nachfrage nach sicheren Cloud-Diensten, zuverlässigen Remote-Netzwerkverbindungen über SSL und Videokonferenzen ist gestiegen - die neue Welt des Homeoffice wird weiter bestehen bleiben.

Diese Krise beweist auch, dass digitale Freiheit nicht selbstverständlich ist. Böswillige Akteure nutzen neue oder bereits etablierte Strukturen als Angriffsfläche um Profit daraus zu schlagen. Jeder kann auf individueller oder kollektiver Ebene davon betroffen sein.

Dies kann das digitale Vertrauen beschädigen. Bei Orange Cyberdefense glauben wir, dass die digitale Welt ein vertrauenswürdiger Ort für Freizeit, berufliche Möglichkeiten und Dienstleistungen sein kann, der das tägliche Leben einfacher, erfolgreicher und erfüllter macht.

Deshalb bemühen wir uns, nicht nur in der Krise sondern auch auf dem Weg in die Zukunft, Verteidigungslinien zu schaffen und die Freiheiten im digitalen Raum zu schützen. Unser Ziel ist es, beim Aufbau einer sichereren digitalen Gesellschaft zu helfen.

Im vergangenen Jahr haben wir durch unsere 16 CyberSOCs/SOCs täglich über 50 Milliarden Ereignisse analysiert, mehr als 35.000 Sicherheitsvorfälle gelöst und mehr als 170 Einsätze zur Bewältigung von Vorfällen geleitet.

Unsere erstklassigen Experten haben all diese einzigartigen Informationen ausgewertet und die wichtigsten Erkenntnisse in diesem Bericht zusammengefasst. Zum Nutzen unserer Kunden und der Cybersecurity Community.

Wir sind stolz und fühlen uns geehrt, jeden Tag mit der Sicherheit der wichtigsten Assets unserer Kunden betraut zu werden, und setzen in allen Bereichen das beste Fachwissen und die beste Technologie ein, um ihr Geschäft zu schützen.

Vielen Dank für Ihr Vertrauen!

Hugues Foulon
Michel Van Den Berghe

Inhaltsverzeichnis

2019 Timeline ▸

COVID-19 & Cybersecurity

Während sich die COVID-19 - Pandemie weltweit immer weiter ausbreitet, versuchen Akteure der Cyber-Kriminalität aus der globalen Gesundheitskrise Kapital zu schlagen, indem sie Malware erstellen oder Angriffe mit einem COVID-19-Thema starten. Diese Art von ausbeuterischem Verhalten des Cyberkriminalitäts-Ökosystems ist jedoch nur ein Teil eines größeren Bildes der Cybersecurity. Orange Cyberdefense veröffentlicht diese Informationen, um die Aufmerksamkeit auf eine Reihe von Fakten zu lenken, die jetzt berücksichtigt werden sollten.

Sie finden den kompletten Report unter www.orangecyberdefense.com/de/covid-19/

Die COVID-19-Pandemie hat die Modelle der Sicherheitsbedrohung in fünf wichtigen Punkten verändert:

Ihre Mitarbeiter sind anfälliger für Social Engineering und Betrug als normal.

Sie haben weniger Kontrolle und Transparenz über die IT-Systeme, die Sie schützen, als Sie es gewohnt sind.

Ihre Benutzer verbinden sich möglicherweise von Systemen und Umgebungen aus, die grundsätzlich unsicher oder schlecht konfiguriert sind.

Möglicherweise haben Sie Systeme für den Remote-Zugang überhastet implementiert, ohne die Zeit zu haben, die Planung und Ausführung nach Ihren Vorstellungen umzusetzen.

Sie, Ihr Team und Ihre Versorger arbeiten möglicherweise mit verminderter Kapazität.

Auswirkungen auf die digitale Welt

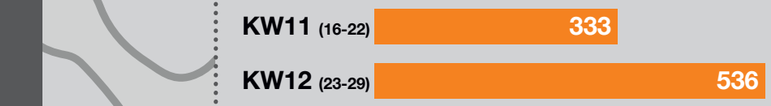
Einige der Tendenzen, die wir während des Lockdowns beobachtet haben:

1. Malware und Phishing unter dem Deckmantel von COVID-19
2. Allgemeine Fehlinformationen/ Fake-News Kampagnen
3. Einige Ransomware-Gruppierungen haben einen "Waffenstillstand" ausgerufen
4. Gezielte Angriffe auf Gesundheitswesen- und Forschungseinrichtungen
5. Erhöhte geopolitische Spannungen, die weitere Cyberkriege entfachen
6. Angriffe gegen Remote Access Technologien und VPN-Gateways
7. Die Sichtbarkeit durch SIEM war beeinträchtigt
8. Die Computeraktivität wurde in die Cloud ausgelagert
9. Beschleunigter Übergang zum E-Commerce
10. Erhöhte permanente Belastung der Internet-Infrastruktur

Der perfekte Köder

Allein am 24. März verfolgte unser CERT-Team in Frankreich 23 einzigartige COVID-19-basierte Phishing-Mails über einen Zeitraum von 24 Stunden. Unser CERT-Team berichtete außerdem, dass Kunden in derselben Woche mehr als 600 potenziell betrügerische E-Mails gemeldet haben, von denen sich 10% als bösartig erwiesen haben.

Mutmaßliche Phishing-Mails von Kunden gemeldet



Die Zahl der bestätigten betrügerischen E-Mails war 4 mal höher als in der Vorwoche.

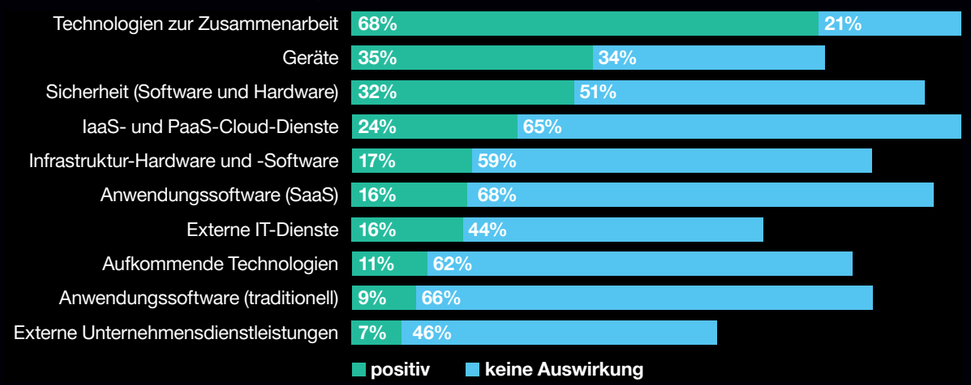
Zusammenfassung der Empfehlungen

Während einer Krise wie COVID-19 empfehlen wir Ihnen, sich auf die folgenden Antworten zu konzentrieren, in der Reihenfolge ihrer Wichtigkeit:

- Einführung von Emergency Response-Verfahren und -Systemen.
- Einrichtung einer Security Support Hotline und Vorbereitung auf die Erweiterung eines Unterstützungsteams.
- Überprüfung von Backup und Disaster Recovery (DR).
- Statten Sie Ihre Benutzer mit den Informationen aus, die sie benötigen, um die richtigen Entscheidungen hinsichtlich Security treffen zu können.
- Sicheren Remote Access bereitstellen.
- Schaffen Sie Sichtbarkeit über Remote Endpoints.

Wie wird COVID-19 die Technologie verändern?

In einer IDC-Umfrage wurden 180 Organisationen in ganz Europa zu den Auswirkungen der Krise auf Technologieinvestitionen befragt.



https://www.idc.com/getdoc.jsp?containerId=EUR146175020

Lehren aus der Krise

Ratschläge sind in Krisenzeiten leicht gesagt. Aber jedes Unternehmen ist anders, und wir werden nicht so tun, als wüssten wir, wie die einzelnen Unternehmen auf ihre individuelle Sicherheitsbedrohung reagieren sollten. Wir möchten jedoch die folgenden Guidelines für Unternehmen anbieten, die die Sicherheitsbedrohung bewerten und sich mit ihrer Reaktion auf die Bedrohung unter Anbetracht der Krise befasst:

1. Verstehen Sie, dass wir uns in einem Zustand erhöhter Bedrohung befanden, die Verwundbarkeit dabei aber nur leicht erhöht war. Wir können zwar die Bedrohung nicht kontrollieren, aber wir können die Verwundbarkeit beeinflussen, also sollten wir uns darauf konzentrieren.
2. Halten Sie sich vor Augen, was sich verändert hat und was nicht. Das Bedrohungsmodell Ihres Unternehmens mag heute ganz anders sein als gestern, oder auch nicht. Wenn es sich nicht geändert hat, dann müssen sich Ihre Strategien und Ihre Handlungen auch nicht ändern.
3. Bilden Sie Partnerschaften, aber vermeiden Sie Mobs. Ihre Lieferanten, Dienstleistungsanbieter und sogar Konkurrenten sitzen alle im selben Boot, gerade in Krisenzeiten. Sie haben vielleicht auch nicht alle Antworten, aber es könnte an der Zeit sein, die Hand auszustrecken und Partner zu finden, die ausgewogene und rationale Ansichten haben und Gemeinschaften zu vermeiden, die Hype und Hysterie verbreiten.
4. Behalten Sie den Kontext im Auge. IT und Internet haben trotz verschiedener Sicherheitsmängel zwanzig Jahre lang überlebt. Es besteht kein Zweifel, dass eine Krisensituation besorgniserregend ist und dass die Gefahr einer grundlegenden Cybersicherheitskrise real ist und nicht ignoriert werden kann. Nichtsdestotrotz handelt es sich um eine medizinische und menschliche Krise. Lassen Sie sich durch den Hype um die Cybersecurity nicht davon ablenken.
5. Arbeiten Sie smart, nicht hart. Sie werden in Zeiten verminderter Möglichkeiten nur sehr wenig erreichen können, daher sollten Sie Zeit und Energie darauf verwenden, sich zu überlegen, was Ihre Hauptanliegen sind, und sich auf diese konzentrieren.

www.orangecyberdefense.com

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Einführung

The state of the threat

“Es wird zu viel für die falschen Dinge ausgegeben. Sicherheitsstrategien wurden auf Furcht und Compliance-Probleme ausgerichtet und verkauft, wobei die Ausgaben eher für wahrgenommene als für echte Bedrohungen getätigt wurden”.

Art Coviello, RSA Chief Exec (2017)

Ein Zermürbungskrieg

Cybersecurity ist ein Problem der Ressourcen. Sowohl der Angreifer als auch der Verteidiger verfügen über begrenzte Ressourcen in Form von Zeit, Geld und Fähigkeiten, die sie strategisch einsetzen müssen, um ihre Ziele zu erreichen.

In einer komplexen und sich entwickelnden Landschaft ist es sehr schwierig, den Unterschied zwischen "wahrgenommenen" und "echten" Bedrohungen zu erkennen. Wie Art Coviello betont, hat dieser Mangel an Gewissheit zu Zweifeln und zu stark angstbestimmten Käufen geführt. Aber was sind die "echten" Bedrohungen? Und wie können wir sie identifizieren und verfolgen, wenn sich die Bedrohungslandschaft im Laufe der Zeit verändert?

Erlauben Sie uns, auf die umfangreiche Datensammlung, die uns zur Verfügung steht, und auf die umfassenden Fähigkeiten und Erfahrungen unserer Spezialisten zurückzugreifen, um Ihnen zu helfen, aus der Vergangenheit zu lernen und, wenn möglich, für die Zukunft zu planen.

Der Stand der Bedrohung ergibt sich aus der Beziehung zwischen drei Hauptkomponenten - strukturelle Kräfte, inflationäre Faktoren und die Evolution der Technologie.

Strukturelle Kräfte

Zu den strukturellen Kräften gehören die systemischen Elemente, die Voraussetzungen und Zwänge schaffen, welche die Bedrohung und unsere Fähigkeit, auf sie zu reagieren, prägen. Diese Faktoren sind in unsere Kontexte und unser Umfeld eingewoben und haben einen grundlegenden Einfluss auf die Form der Bedrohung und unsere Reaktionsfähigkeit.

Ein Beispiel für eine solche strukturelle Kraft ist die Innovation durch Kriminelle. Es ist nicht das "Cyber" in der Cyber-Kriminalität, das sich entwickelt; es ist das "Verbrechen". Neue Wege zur Monetarisierung bestehender Angriffsmethoden - zum Beispiel durch Cryptomining und Lösegeldforderungen - verändern die Art der Bedrohung in einem sehr schnellen Tempo und formen so unsere Bedrohungsmodelle immer wieder neu.

Die wichtigsten Trends, die CISOs beeinflussen:

- Vorschriften und Gesetze zur Cybersicherheit;
- Verantwortung der Geschäftsleitung vs. mangelnde Sichtbarkeit; und
- Marktknappheit (Zunahme der Anforderungen vs. steigende Nachfrage nach Talenten).

Nadav Shatz /
Director of Advisory, Consulting and Architecture,
Orange Cyberdefense

Ein weiteres Beispiel ist, dass Cyberabwehr zu einer Kernfunktion des Unternehmens geworden ist und leitende Angestellte und Vorstände sich viel stärker mit dem Thema Cybersecurity auseinandersetzen. Aber die Vorstände, die sich in erster Linie mit der Regulierung, der Einhaltung von Vorschriften und ihrer treuhänderischen Verantwortung als Direktoren befassen, üben nun auch Druck auf die CISOs aus, damit diese ihre Arbeitsweise weiterentwickeln. Dies lenkt die CISOs davon ab, die Bedrohung zu verstehen und sich mit ihr auseinanderzusetzen, da sie sich stattdessen darauf konzentrieren, die Anforderungen des Vorstands zu verstehen und zu erfüllen.

Inflationäre Faktoren

Wie wir festgestellt haben, geht die Bedrohungslandschaft, mit der wir heute konfrontiert sind, zuallererst aus einem Kontext hervor, der von mächtigen strukturellen Kräften geprägt ist. Diese Kräfte können militärischer, politischer, wirtschaftlicher, sozialer oder rechtlicher Natur sein und ihren Ursprung auf nationaler oder internationaler Ebene haben.

Wenn die Form der Bedrohungslandschaft erst einmal definiert ist, werden die Herausforderungen, vor denen wir stehen, durch ebenso mächtige und noch weniger kontrollierbare "inflationäre Faktoren" verstärkt.

Eine Reihe von inflationären Faktoren sind das Ergebnis der Ambivalenz, die Regierungen weltweit hinsichtlich einer grundlegenden Lösung des Sicherheitsproblems empfinden, und der anhaltenden Investitionen der Regierungen in den Aufbau und die Nutzung ausgefeilter Hacker-Tools und -Techniken zur Verfolgung ihrer politischen Ziele. Wir glauben, dass die Investitionen der Streitkräfte in Computer-Hacking der bedeutendste Faktor in diesem Bereich sind.

Da Konflikte zwischen Nationalstaaten im Cyberspace unweigerlich an Ausmaß und Intensität zunehmen, ist der wichtigste Punkt, den es zu beachten gilt, dass diese Konflikte im Internet auftreten, welches wir alle teilen. Ihre Auswirkungen können nicht auf "staatliche" Ziele beschränkt werden, und der Rest von uns wird unweigerlich auf die eine oder andere Weise von diesen Konflikten betroffen sein. Betrachten Sie es als Kollateralschaden.

Letztendlich werden Technologie, Ausbildung, Fähigkeiten und Erfahrung der Regierung ihren Weg in das zivile Ökosystem finden, wo sie eine höchst störende Wirkung haben können, wie die Ausbrüche von WannaCry und notPetya deutlich gezeigt haben. Umfang und Ausmaß von staatlich finanzierten Initiativen haben das Potenzial, alles, was wir in unserer Branche für "wahr" halten, völlig zu untergraben.

Aus der Perspektive der Cyber-Verteidigung sind diese mächtigen geopolitischen Kräfte wie das Wetter. Sie haben einen enormen Einfluss auf unsere tägliche Realität. Wir können diese Kräfte zwar beobachten und sogar versuchen, sie vorherzusagen, aber wir haben keine Möglichkeit, sie zu kontrollieren. Wir haben hier nur die Wahl, sie zu observieren und unsere eigenen Strategien entsprechend daran zu orientieren.

In der heutigen Welt findet kein einziger militärischer Einsatz statt, ohne dass die Fähigkeit zur Cyberverteidigung, sei es im Bereich des Geheimdienstes, bei psychologischen Operationen, bei der Zielbestimmung, bei der Zerstörung oder bei der Auswertung nach einem Streik, beeinträchtigt wird.

Laurent Célérier / EVP Technology & Marketing,
Orange Cyberdefense

Former senior officer, French Ministry Of Defense

Evolution der Technologie

Es liegt auf der Hand, dass die Entwicklung der Technologie zusammen mit den neuen Geschäftsmodellen und Prozessen, die sie ermöglicht, einen bedeutenden Einfluss auf die Bedrohungslandschaft haben würde. Sowohl der Angreifer und der Verteidiger selbst sind von den kleinsten Änderungen an den Systemen und Werkzeugen, die beide Seiten verwenden, betroffen. Es gibt einige konsistente Prinzipien, die beschreiben, wie sich die technologische Evolution auf den Stand der Bedrohung auswirkt.

Ein solches Prinzip besagt, dass neue Technologien für die meisten Unternehmen alte Technologien selten vollständig ersetzen, sondern sie lediglich ergänzen. Daher wird ein Unternehmen im Laufe der Zeit mit einem tiefen Pool von Sicherheits-"Schulden" belastet, die nie verschwinden, sondern eher zunehmen. Wir können mit Zuversicht behaupten, dass die Herausforderungen, mit denen wir gestern noch zu kämpfen hatten, uns wahrscheinlich auch morgen noch viel abverlangen werden, und dass neue und sich entwickelnde Technologien das Risiko wahrscheinlich nicht verringern, sondern eher neue Bedrohungen hinzufügen werden.

Ein offensichtliches Beispiel für das obige Prinzip ist die Einführung von 5G. Die neue Technologie ist zweifellos sicherer als ihre Vorgänger und verspricht, ein bedeutender Wegbereiter für Technologien und Geschäftsmöglichkeiten der nächsten Generation zu sein. Sie wird aber zweifellos auch die Sicherheitsschulden vervielfachen, die die Technologieindustrie aufbaut, um ständig verschiedene neue Formen von Technologien zu entwickeln, vermarkten und zu verkaufen. IoT-Systeme werden offensichtlich bereits von denselben Sicherheitsproblemen geplagt, die Desktop-Computer seit Jahrzehnten kennzeichnen, aber sie bringen auch ihre eigenen Herausforderungen mit sich (wie z.B. das Patchen von Firmware in großem Maßstab per Fernzugriff). Diese Probleme werden durch den Umfang der IoT-Implementierungen massiv verstärkt.

Vom Standpunkt der Cyberabwehr aus gesehen ist die Technologie jedoch etwas, über das wir Kontrolle ausüben können.

Die Auswirkungen einer neuen Technologie werden auf kurze Sicht immer über- und auf lange Sicht unterschätzt.

Wir wissen nicht, was sich ändern wird, aber wir können zuversichtlich erahnen, was unverändert bleiben wird.

Etienne Greeff / CTO Orange Cyberdefense

Wir können uns dafür entscheiden, eine neue Technologie nicht zu übernehmen, und wir können entscheiden, wann und wie wir andere zur Bewältigung neu auftretender Sicherheitsbedrohungen einsetzen.

Da diese Bemühungen vollständig unter unserer Kontrolle stehen, macht es für uns durchaus Sinn, dabei auf anerkannte bewährte Praktiken zurückzugreifen.

Abwägung unserer Optionen

Unter erneutem Nachdenken über die drei Schlüsselfaktoren, die die entstehende Bedrohungslandschaft ausmachen, überlegen wir, wie wir als Cyberverteidiger diese Kräfte zu unserem eigenen Vorteil kontrollieren oder beeinflussen können.

Da es nur ein einziges beitragendes Element der entstehenden Bedrohungslandschaft gibt, über das wir wirklich die Kontrolle haben - das technologische Element - muss dies eindeutig unser unmittelbarer, kurzfristiger Schwerpunkt sein. Dies erfordert den intelligenten Einsatz von Technologie, Menschen und Best-Practice-Prozessen, um Bedrohungen gegenüberzutreten und Risiken zu reduzieren.

Obwohl unsere Anstrengungen auf technologischer Ebene eindeutig notwendig sind, haben die drei Elemente leider nicht alle den gleichen Einfluss auf den sich abzeichnenden "state of the threat".

Structurelle Kräfte
Systemische Kräfte, die Voraussetzungen und Zwänge schaffen, welche die Be drohung und unsere Reaktion darauf bestimmen

Beeinflussen
Wir können diese Faktoren nicht kontrollieren, aber beeinflussen. Einfluss ist auf lange Sicht der weitreichendste Weg, Bedrohungen zu begegnen.

Inflationäre Kräfte
Die Bedrohung ergibt sich aus politischem, wirtschaftlichem, sozialem, rechtlichem und regulatorischem Kontext

Beobachten und orientieren
Diese Kräfte sind wie das Wetter: Sie haben einen enormen Einfluss, aber wir können sie nicht kontrollieren. Wir haben nur die Wahl, sie zu beobachten und uns entsprechend anzupassen.

Evolution der Technologie
Mit der Entwicklung der Technologie verändert sich auch die Bedrohung

Steuerung
Wir können die Größe unserer Angriffsfläche verringern, und Schwachstellen finden und eliminieren. Diese Möglichkeiten stehen uns offen, daher ist es sinnvoll, sie bestmöglich zu nutzen.

> Die bösen Jungs werden weiter von Innovation getrieben sein. Wir müssen akzeptieren, dass es Verstöße geben wird, und über Detection und Response nachdenken.
>
> Stefan Lager / SVP Global Service Lines, Orange Cyberdefense Nordics

Die Bedrohungslandschaft wird mehr von den Faktoren beeinflusst, die wir nicht kontrollieren können, als von den Faktoren, die wir kontrollieren. Dies deutet darauf hin, dass wir zwar unbedingt unsere Technologie, Menschen und Verfahren weiter verbessern müssen, dass wir aber auch akzeptieren und antizipieren müssen, dass dies allein nicht ausreichen wird, um angesichts aktueller und "echter" Bedrohungen das von uns gewünschte Maß an Widerstandsfähigkeit zu erreichen.

Eine Vertrauenskrise

Man könnte argumentieren, dass die Rolle der Security innerhalb der Technologie darin besteht, Vertrauen zu schaffen und durchzusetzen. Die drei Säulen der "CIA-Triade" - Vertraulichkeit, Integrität und Verfügbarkeit - definieren für uns, wie das durchgeführt werden sollte: indem wir sicherstellen, dass die von uns verwendeten Daten und Systeme vertrauenswürdig genug sind, um Geheimnisse zu wahren, Genauigkeit zu gewährleisten und verfügbar zu sein, wenn wir sie brauchen. Wenn die Sicherheit versagt, ist Vertrauen kompromittiert. Wenn das Vertrauen einmal verloren ist, ist es sehr schwierig, es wiederzugewinnen. In der Tat ist das Vertrauen in die Systeme, von denen unsere Unternehmen, unsere Gesellschaften und unser Leben abhängen, so wichtig, dass es einer Krise gleichkäme, das Vertrauen in eine Schlüsseltechnologie zu verlieren.

Die Lektion für diejenigen, die in der Technologie tätig sind, ist einfach und klar: Unsere Interessenvertreter müssen in der Lage sein, den Systemen und Daten, für die wir verantwortlich sind, zu vertrauen.

Wenn es zu Angriffen, Verstößen und Gefährdungen kommt, wird dieses Vertrauen beschädigt, und die Folgen sind weitreichend. In einem komplexen System mit mehreren Faktoren, die wir nicht kontrollieren, können wir nicht verhindern, dass Krisen entstehen.

Wir können sie jedoch im Keim ersticken, und dazu brauchen wir gute Sichtbarkeit, Früherkennung und klare und zuversichtliche Reaktionsmöglichkeiten. Über die Erhaltung des Vertrauens hinaus müssen wir uns darauf konzentrieren, das Vertrauen wiederherzustellen, wenn schlimme Dinge passiert sind. Detection, Response und Recovery spielen eine wesentliche Rolle.

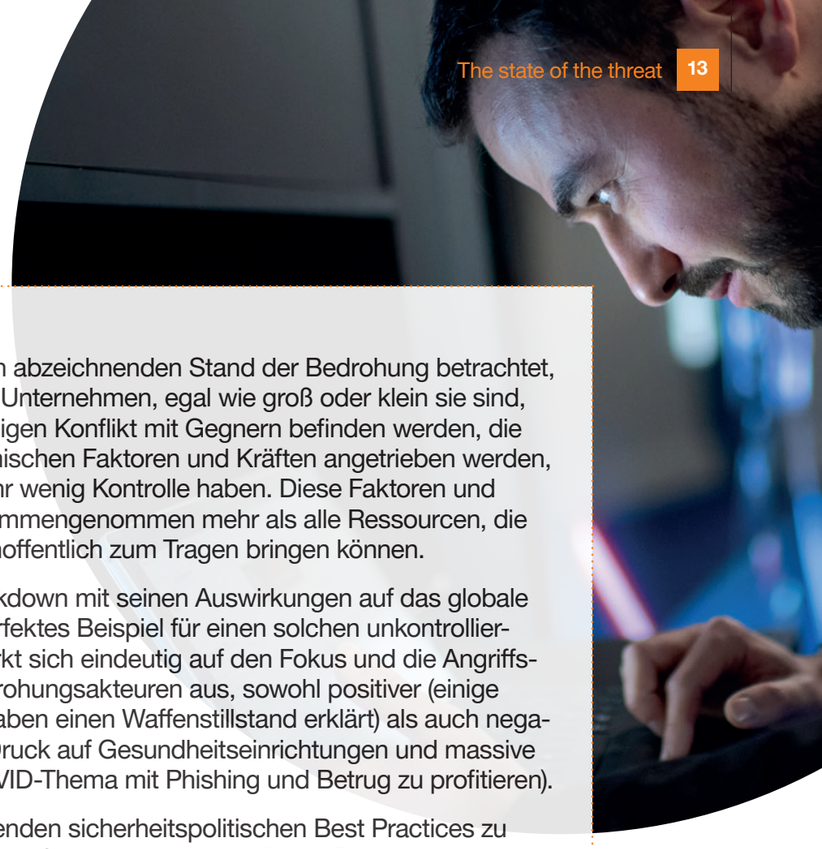
Die Balance halten: Erkennung, Reaktion, Wiederherstellung

Unsere Paradigmen müssen sich eindeutig ändern, und Dominic White, CTO der Elite Attack and Penetration Testing Unit von Orange Cyberdefense, gibt uns einen Einblick, in welche Richtung wir uns bewegen müssen.

> Wenn sie uns entdecken, verbrennen sie uns, und das hat Konsequenzen. Angreifer haben auch einen Chef und ein Budget.
>
> Dominic White / CEO, SensePost

Diese Einsicht eines Teams erfahrener Angreifer veranschaulicht, dass die verschiedenen präventiven Kontrollen, die wir einführen, dem Angreifer zwar Kosten verursachen können, dass aber eine wirksame Detection und Response durch eine Elite Attack and Penetration Testing Unit sie wirklich zurückwerfen kann. Aus dieser Lektion gehen unsere Überzeugungen von "Engagement" hervor: Der Gegner kann nicht länger an den Toren zurückgehalten werden.

Wir müssen uns darauf einstellen, dass der Gegner hinter unseren Grenzen und auf unseren Systemen aktiv ist. Wir müssen sie dort finden und ihnen dort entgegenwirken, oft System für System, bis sie vertrieben werden. Wie alle früheren Sicherheitsdoktrinen ist auch "Detect, Respond & Recover" keine Wunderwaffe. Es kann nicht isoliert eingesetzt werden, und es wird die systemischen strukturellen und inflationären Kräfte, mit denen wir konfrontiert sind, nicht überwinden. In einer heutigen Zeit, die den Angreifer immer noch überwältigend begünstigt, ist dies jedoch eine notwendige taktische Reaktion.



Fazit

Wenn man den sich abzeichnenden Stand der Bedrohung betrachtet, wird deutlich, dass Unternehmen, egal wie groß oder klein sie sind, sich in einem ständigen Konflikt mit Gegnern befinden werden, die von großen, systemischen Faktoren und Kräften angetrieben werden, über die wir nur sehr wenig Kontrolle haben. Diese Faktoren und Kräfte wiegen zusammengenommen mehr als alle Ressourcen, die wir als Verteidiger hoffentlich zum Tragen bringen können.

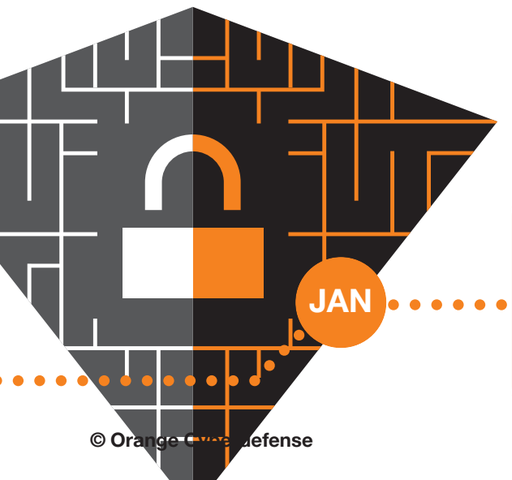
Der COVID-19-Lockdown mit seinen Auswirkungen auf das globale Geschäft ist ein perfektes Beispiel für einen solchen unkontrollierbaren Faktor. Er wirkt sich eindeutig auf den Fokus und die Angriffsschemata von Bedrohungsakteuren aus, sowohl positiver (einige Hacker-Gruppen haben einen Waffenstillstand erklärt) als auch negativer Art (erhöhter Druck auf Gesundheitseinrichtungen und massive Versuche, vom COVID-Thema mit Phishing und Betrug zu profitieren).

Ohne die grundlegenden sicherheitspolitischen Best Practices zu vernachlässigen, die erforderlich sind, um diesen Bedrohungen entgegenzuwirken (ohne die sie uns einfach überwältigen würden), müssen wir erkennen, dass Angriffe, Gefährdungen und Verstöße unvermeidlich sind, und uns darauf vorbereiten, unseren Gegner aktiv und kontinuierlich hinter den traditionellen Grenzen unseres Umfelds zu bekämpfen.

Ausgereifte und effektive Detection- und Response-Fähigkeiten sind nicht nur eine existenzielle Voraussetzung angesichts der gegenwärtigen Bedrohungen, sondern wirken auch einigen der Vorteile entgegen, die unseren Gegnern einen systemischen Vorteil verschaffen. Nämlich die Minimierung ihres Überraschungsmomentes, die Zufügung von Kosten und Konsequenzen für ihre Fehler und die Verlängerung der Zeit, die sie zum Lernen und Verbessern benötigen, bei gleichzeitiger Reduzierung der Zeit für uns, das Gleiche zu tun.

Eine wirksame Detection, Response und Recovery ist entscheidend, um das Vertrauen wiederherzustellen, wenn der unvermeidliche Angriff zustande kommt.

Die Bedrohung entwickelt sich weiter, ein Angriff ist unvermeidlich, Engagement ist unerlässlich.



Z-WASP ermöglicht es Hackern den E-Mail-Schutz von Office 365 zu umgehen

Forscher von Avanan setzten erfolgreich nicht druckbare, breitenlose HTML-Zeichen ein, um Office 365 daran zu hindern, bösartige Links zu erkennen. Dies funktioniert auch dann, wenn MS-Advanced Threat Protection (ATP) aktiviert ist [t1].

Hacktivist zu 10 Jahren verurteilt für DDoS-Angriff auf Krankenhaus

Martin Gottesfeld hatte 2014 über ein Botnetz von 40.000 Routern das Boston Children's Hospital und eine andere Einrichtung angegriffen, angeblich um gegen die missbräuchliche Behandlung von Justina Pelletier zu protestieren [t2].

Die Fondation du Patrimoine und der Notre-Dame Brand

Nachdem die Dächer der Kathedrale Notre-Dame de Paris am 15. April 2019 abgebrannt waren, sah sich die Fondation du Patrimoine einer weiteren Krise gegenüber. Vom Staat ermächtigt, Solidaritätsfonds für den Wiederaufbau des Bauwerks zu sammeln, wurde diese Einrichtung schnell von einem Problem überwältigt, mit dem sie nicht gerechnet hatte: der Zunahme betrügerischer Spendenaktionen und der Registrierung von parasitären Domainnamen.

"Viele Websites versuchten, sich als legitime Spendensammler auszugeben, und die Seite der Heritage Foundation war zwei Stunden lang offline [...] Es war von einer seltenen Größenordnung, so etwas hatte ich noch nie gesehen. Die Stiftung war nicht bereit, sich einer solchen Situation zu stellen."

Jean-Michel Livowski, DPO, Fondation du Patrimoine

Kennzahlen der Krisenbewältigung:

- ca. 50 Tage Monitoring
- Ungefähr 20.000 Hinweise, die an den Krisenstab weitergeleitet wurden
- Knapp 400 identifizierte Parallel-Pools wurden den Behörden gemeldet
- Mehr als 20 Domainnamen unter Beobachtung

"Die von der Heritage-Stiftung lancierte Spendensammlung war mit über 220.000 Einzelspendern ein großer Erfolg. Diese historische Mobilisierung, die akut und in Rekordzeit durchgeführt wurde, hätte ohne die Zusammenarbeit und die Arbeit der Orange Cyberdefense keinen Erfolg gehabt. Die Wachsamkeit und die Warnungen der Orange Cyberdefense-Teams ermöglichten es uns, in einem Krisenkontext, mit dem die Stiftung noch nie zuvor konfrontiert war, ruhig und effizient zu arbeiten.

Orange Cyberdefense war einer der Hauptakteure bei der erfolgreichen Mobilisierung von Tausenden von Spendern."

Guillaume Poitrinal, President der Heritage-Stiftung

Besorgt über die Situation und eine mögliche Verschärfung der Angriffe aufgrund des bevorstehenden Osterwochenendes nahm die Presse am Abend des 19. April, dem Vorabend eines langen Wochenendes, das böswilligen Akteuren helfen würde, Kontakt mit Orange Cyberdefense auf. Das Incident Response Team (CSIRT) und die Alerts Center (CERT)-Teams von Orange Cyberdefense beschlossen, unverzüglich ein Krisenmanagementsystem einzurichten.

Krisenmanagement in Rekordzeit

Während die Spenden einströmten, wurden die ersten Maßnahmen von der Heritage Foundation ergriffen, darunter die Einrichtung einer offiziellen Webseite, die den Spenden gewidmet ist, unterstützt durch eine Kommunikationskampagne, die von den verschiedenen Medien und sozialen Netzwerken aufgegriffen wurde. Diese sowie die Websites von Notre-Dame de Paris und der Fondation du Patrimoine wurden von Analysten von Orange Cyberdefense beobachtet.

Zusätzlich zu dieser ersten Sicherheitsmaßnahme gab es auch ein Überwachungssystem für:

- Domänennamen
- Mobile Anwendungen
- Profile in sozialen Netzwerken
- Das offizielle Fundraising auf den spezialisierten Plattformen

Ein Krisenstab sendete über ein Extranet Warnungen in Echtzeit an die Manager, Anwälte und Justizbehörden der Heritage Foundation.

Sara Puigvert
EVP Global Operations
Orange Cyberdefense

Franz Härtl
Head of Global Content Marketing
Orange Cyberdefense

CyberSOC Statistiken

Das ist passiert

Der Schutz von IT-Assets, -Systemen und -Infrastrukturen, um Geschäfte sicher zu ermöglichen, ist unser tägliches Brot. Wenn wir für unsere Kunden auf der ganzen Welt Sicherheitsvorrichtungen, Endpoints, Cloud-Anwendungen, OT-Umgebungen und Netzwerke überwachen, sehen wir vieles von dem, was in den Nachrichten berichtet wird, mit eigenen Augen.

Ein kontinuierlicher Datenstrom durchläuft unsere 10 CyberSOCs und 16 SOCs. Wie bereits in unseren früheren Annual Security Reports haben wir beschlossen, diese Daten zu vertiefen und die Zahlen zu extrapolieren, um ein besseres Verständnis für die sich ständig weiterentwickelnden Bedrohungslandschaft zu erhalten.

Als Teil des neuen Security Navigators können wir Ihnen also wieder ein sehr reales Bild der Ereignisse und Trends des vergangenen Jahres aus erster Hand vermitteln.

Diese Daten wurden gesammelt, bevor COVID-19 begann sowohl die Geschäfts- als auch die Bedrohungslandschaft zu beeinflussen, und können als wichtige Grundlage für den Vergleich mit zukünftigen Daten dienen.

Über die Daten

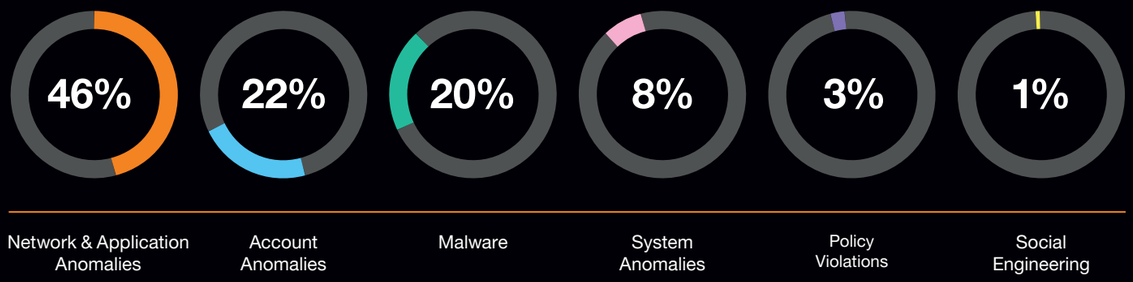
- **Gesamtzahl der analysierten Ereignisse: 263.109**
- **Von diesen Ereignissen werden 11,17% (29.391) von Orange Cyberdefense*-Datenklassifikationen als Incidents betrachtet**
- **Analysezeitraum: Vollständige Daten für das gesamte Jahr 2019**
- **Datenquellen: Firewalls , Verzeichnisdienste, Proxy, Endpoint, EDR, IPS, DNS, DHCP, SIEM und unsere Managed Threat Detection Plattform**

*Inklusive Alerts aus einem Teil unseres operativen Bereichs für diese Sonderausgabe

Funnel:
Alerts to Incidents

263,109
Alerts • Use Cases • Events

29,391
11.17% Security Incidents



Arten von Incidents

Im Jahr 2019, haben wir die folgenden Arten von Vorfällen feststellen können:

Network & Application Anomalies, wie Tunneling, IDS/IPS-Warnungen und andere Angriffe im Zusammenhang mit Netzwerkverkehr und -anwendungen.

Account Anomalies, wie z.B. Brute-Force-Angriffe, Wiederverwendung von Credentials, Lateral Movement, Erhöhung von Privilegien oder Ähnliches.

Malware ist bösartige Software wie Ransomware.

System Anomalies sind Ereignisse, die direkt mit dem Betriebssystem und den Komponenten um das Betriebssystem herum zusammenhängen, wie z.B. Treiber, die nicht mehr funktionieren, oder Dienste, die unerwartet beendet werden.

Policy Violations, wie z.B. die Installation nicht unterstützter Software oder der Anschluss eines nicht autorisierten Geräts an das Netzwerk.

Social Engineering ist jeder Versuch, Benutzer zu täuschen; einschließlich, aber nicht beschränkt auf, Phishing und Spoofing.

Gesamtzahlen

Im Vergleich zu unserem vorherigen Bericht verzeichneten wir eine Zunahme an Warnmeldungen. In diesem Jahr hatten wir mehr Onboardings, sodass diese Diskrepanz erwartet wurde. Erstaunlicherweise ist aber die Zahl der Ereignisse, die wir als sicherheitsrelevant identifiziert haben, stärker gestiegen als erwartet.

Von den insgesamt 263.109 Ereignissen identifizierten wir 11,17% (29.391) als verifizierte Sicherheitsvorfälle. Im Vorjahr lag diese Rate bei 8,31%, d.h. wir verzeichneten einen Anstieg von 38%. Das ist recht signifikant, wenn man bedenkt, dass die Gesamtzahl der Alerts um weniger als 3% gestiegen ist.

Diese Veränderung des Verhältnisses lässt sich zum Teil durch eine bessere Feinabstimmung der Plattform zur Vermeidung von Fehlalarmen in Zusammenarbeit mit unseren Kunden erklären. Dennoch ist es eine Tatsache, dass die Zahl der Sicherheitsvorfälle erheblich zugenommen hat. Angreifer ergreifen jede Gelegenheit, um eine Schwäche auszunutzen.

Have you been pwned?

Ein weiterer Trend, den wir für signifikant halten, ist die Zunahme von Account Anomalies. Im vorigen Bericht wurden 15% unserer Vorfälle als Kontoanomalien eingestuft, und sie haben somit Platz drei belegt. In diesem Jahr sind sie mit 22% auf dem zweiten Platz gelandet. Wie kam es dazu?

Eine mögliche Erklärung wäre die ungewöhnliche Häufigkeit und das schiere Ausmaß der diesjährigen Datenlecks. Wie Sie in mehreren Punkten der Timeline von 2019 nachlesen können, wurden buchstäblich Hunderte von Millionen Konten und Zugangsdaten veröffentlicht und im Darknet verkauft. Wenn man den Fakt hinzuzieht, dass Menschen Passwörter gerne mehrfach verwenden, besonders wenn sie alle 100 Tage geändert werden müssen, ist es offensichtlich, dass wir hier auf Probleme stoßen.

Der Schlüsselbegriff lautet "Credential Stuffing". Und dieser Anstieg ist vielleicht nur die Spitze des Eisbergs, denn selbst Kriminelle brauchen einige Zeit, um Daten in diesem Umfang zu verarbeiten und zu missbrauchen . Mehr über Datenlecks, ihre Ursachen und Auswirkungen können Sie im Kapitel "Datenlecks überall" nachlesen.

Social Engineering ist weiterhin schwer aufzuspüren

Statistiken über Social Engineering sind heikel. Social Engineering umfasst alle Arten von Aktivitäten, die gewöhnlich dem eigentlichen Angriff vorausgehen. Es beginnt mit der Recherche von Zielkonteninhabern oder wichtigen Positionen des Managements in verschiedenen sozialen Medien wie LinkedIn oder Facebook. Die Ziele könnten zum Beispiel anschließend so manipuliert werden, dass sie Details über Systeme, Netzwerkeinrichtungen oder sogar Zugangsdaten durch Telefonanrufe von falschen Servicemitarbeitern preisgeben.

All dies kann außerhalb des Firmenumkreises geschehen und liegt damit außerhalb unserer Verfolgungsmöglichkeiten. Threat Intelligence kann in einigen Fällen helfen, solche Vorkommnisse zu identifizieren, aber im Allgemeinen sehen wir nur die Ergebnisse.

Schäden, die durch Social Engineering entstehen, könnten immer noch verhindert werden, je nach Art und Raffinesse des tatsächlichen Angriffs. Allerdings werden resultierende Vorfälle wahrscheinlich in die jeweiligen Kategorien wie Account Anomalies oder Malware eingeordnet, auch wenn sie eine unmittelbare Auswirkung von Social Engineering sind.

Kritische Schwachstelle in der Online-Buchungsplattform "Amadeus" behoben: Fast die Hälfte aller Fluggesellschaften weltweit sind betroffen

Lediglich die Eingabe einiger einfacher Befehle in den Browser ermöglichte es, Datensätze von Passagieren sowie die Flugdaten, Namen und andere persönliche Informationen zu erhalten [t3].

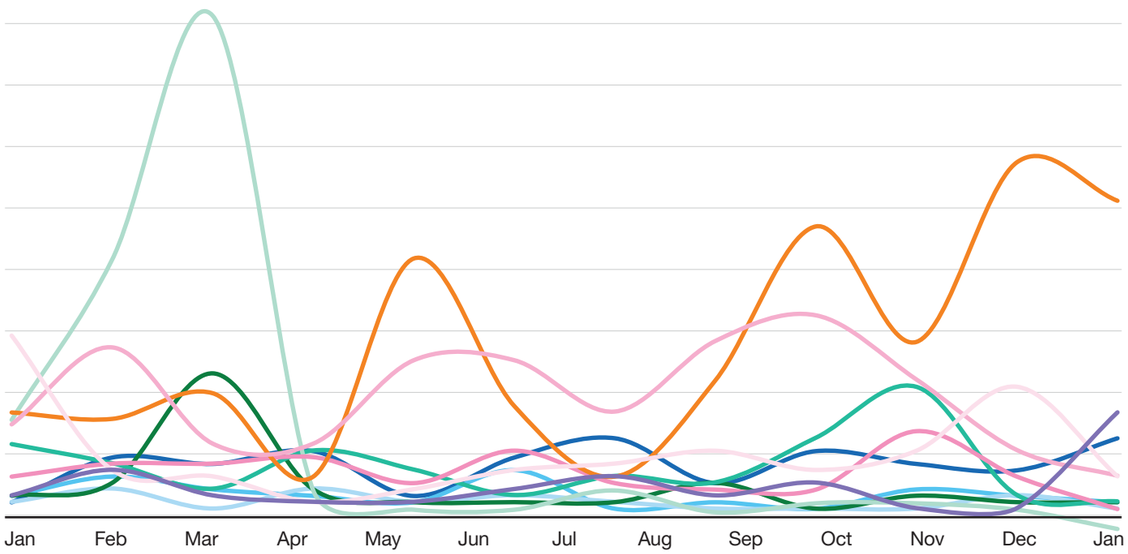
Endpoint-Schutz funktioniert

Eine weitere bemerkenswerte Veränderung, die wir beobachtet haben, ist, dass die Malware-Vorfälle deutlich zurückgegangen sind. Zuvor hatten wir 45 % der Incidents als Malware klassifiziert. Im Jahr 2019 sank dieser Anteil auf 22%. Gleichzeitig stiegen die Netzwerk- und Anwendungsanomalien von 36% auf 46%, was sie zum neuen Spitzenreiter im Jahr 2019 macht.

Bedeutet das, dass Malware keine Bedrohung mehr darstellt? Im Allgemeinen nicht, aber es zeigt, dass Endpoint-centered Prevention das Risiko deutlich verringern kann. Was wir hier sehen, ist sehr wahrscheinlich das unmittelbare Ergebnis der Next-Gen Endpoint Protection. KI-basierte Lösungen gibt es zwar schon seit einiger Zeit, aber ihre Verbreitung hat einige Zeit in Anspruch genommen. Jetzt haben immer mehr Kunden begonnen, in den präventiven Next-Gen Endpoint-Schutz zu investieren. Und wir sehen die Ergebnisse ganz deutlich: Malware verliert schnell an Bedrohlichkeit und fällt nach Account Anomalies zurück auf den dritten Platz.

Zwar stellen ausgereifte Malware und APTs, die bei gezielten Angriffen eingesetzt werden, immer noch eine ernstzunehmende Bedrohung dar, doch das Qualifikationsniveau der durchschnittlichen Cyberkriminellen entspricht nicht mehr der aktuellen Endpoint Protection. Und das sind gute Nachrichten.

Malware Trends im Überblick



Malware Trends

Betrachtet man die allgemeinen Malware-Trends, fallen einige auffällige Muster auf. Die ersten beiden bemerkenswerten Tendenzen sind der Rückgang der Angriffsaktivitäten Anfang April, Mitte Juli und Anfang Dezember. Diese sind wahrscheinlich auf etwas zurückzuführen, das wir bereits in den vergangenen Jahren beobachtet haben: Mit der Professionalisierung der Cyberkriminellen sehen wir, dass sie eine „9 to 5“-Mentalität annehmen. So merkwürdig dies auch erscheint: Hacker nehmen inzwischen regelmäßig Urlaub. Dies könnte den Rückgang erklären, als sich die Zahl der Angriffe aufgrund der Osterferien sowie der Sommerferien und Weihnachten am Ende des Jahres verringerte.

Ransomware hatte ihre Höhen und Tiefen, bleibt aber weiterhin eine beliebte Angriffsform. Bei Mining ist das anders. Während beide Angriffstypen zu Beginn des Jahres einen Anstieg verzeichneten, gingen die Mining-Angriffe zurück und blieben ab April auf einem niedrigen Stand. Auch die Ransomware-Attacken gingen im April zurück, stiegen jedoch im Mai, Oktober und Dezember auf neue Höchststände. Bemerkenswert ist auch, dass die Preise für Monero[2.1], Ethereum[2.2], Litecoin[2.3] und Bitcoin[2.4] im Frühsommer einen neuen Höchststand erreichten, aber es gab so gut wie keine Auswirkungen auf die Häufigkeit der Mining-Angriffe, während wir zuvor gesehen hatten, dass Mining-Angriffe dem Handelswert der Kryptowährungen folgten. Dies deutet darauf hin, dass Cryptomining als Bedrohung endgültig verschwunden ist und in weit verbreiteten Kampagnen voraussichtlich nicht wiederkehren wird.

„Collection #1“: 773 Mio. Datensätze im Darknet gefunden

Der australische Forscher Troy Hunt entdeckte eine riesige Sammlung von Anmeldedaten (E-Mail-Adressen und Passwörter). Die Aufzeichnungen stammen aus mehreren verschiedenen Datenschutzverstößen [t4].

Altran Technologies von Cyber-Angriff betroffen, der Unternehmen in mehreren europäischen Ländern beeinträchtigt

Das französische Ingenieur-Beratungsunternehmen war offenbar von einer gezielten Kampagne betroffen, die Unternehmen in mehreren europäischen Ländern traf [t5].

GandCrab/Ursnif

Vorsicht bei Word-Makros: Ursnif ist ein Trojaner, der kritische Daten exfiltriert, während GandCrab eine klassische Ransomware ist. Beide verbreiten sich über Phishing-E-Mails mit bösartigen Word-Anhängen [t6].

Attacke auf multinationales Joint Venture Airbus

Airbus und seine Zulieferer sind von einer ganzen Reihe von Angriffen betroffen, die darauf abzielen, geistiges Eigentum zu stehlen [t7].

FEB

$145 Millionen verloren, CEO mit einzigem Passwort verstorben

QuadrigaCX, die größte Bitcoin-Börse Kanadas, behauptet, den Zugang zu ihren Offline-Speicherbörsen verloren zu haben, da die einzige Person, die Zugang zu diesen hatte, der CEO und Gründer Gerry Cotton war. Dieser war im Dezember unerwartet verstorben [t8].

E-Scooter Passwort-Schwachstelle erlaubt lebensgefährliche Hacks

Der Elektroroller M365 von Xiaomi wird mit einer anscheinend anfälligen Bluetooth-App geliefert. Da der Roller das Passwort nicht validiert, können Angreifer aus bis zu 100m Entfernung die Bremsen betätigen, beschleunigen oder den Roller ausschalten [t9].

Secure-E-Mail-Anbieter VFEmail.net komplett gelöscht

Mit einem katastrophalen Cyberangriff zerstörten Hacker sämtliche Daten sowohl auf den Primär- als auch auf den Backup-Servern vollständig. Dazu gehörte die gesamte Infrastruktur mit E-Mail-Hosts, virtuellen Maschinen und einem SQL-Server-Cluster. Dies war rein destruktiv, es gab keine Lösegeldforderung [t10].

Hacker verkauft 839 Mio. Accounts im Darknet

Hacker “Gnosticplayers” veröffentlichte drei Runden mit Konten von Dutzenden von gehackten Websites und Diensten auf Dream Market, die zusammen 839 Millionen Datensätze ergeben. Viele der Websites wussten nicht einmal, dass sie gehackt worden waren [t11].

Größe des Unternehmens

Das Gesamtbild hat sich etwas verändert. Betrachtet man die früheren Zahlen, so war die kleinste Veränderung, dass 9,72% der Vorfälle in kleinen Unternehmen stattfanden. Das ist ein geringfügiger Anstieg gegenüber den 8% des letzten Berichts.

Eine bedeutende Verschiebung gab es bei mittleren und großen Organisationen. Im vergangenen Jahr stellten wir fest, dass die großen Akteure bei weitem am stärksten betroffen waren. Im Allgemeinen gilt nach wie vor, dass die meisten Vorfälle sich in Unternehmen mit mehr als 10.000 Beschäftigten ereignen.

Aber was wir dieses Mal auch beobachten konnten, ist ein dramatischer Anstieg der Angriffe auf mittelständische Unternehmen. Im Jahr 2019 verfolgten wir 31% der verzeichneten Vorfälle in diesem Sektor, was einen deutlichen Anstieg gegenüber der vorherigen 19% bedeutet. Gleichzeitig gingen die Vorfälle in großen Organisationen von 73% auf 58,8% zurück.

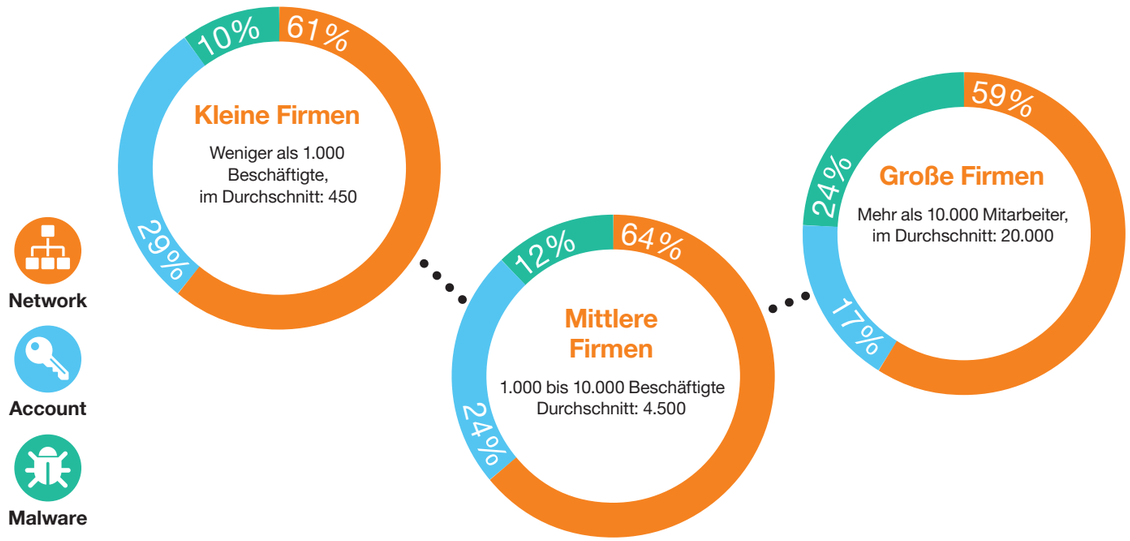
Offenbar haben die Bedrohungsakteure ihren Schwerpunkt teilweise verlagert und zielen nun auf mittelständische Unternehmen mit 1.000-10.000 Beschäftigten, viel mehr als zuvor beobachtet.

Incident-Verteilung nach Firmengröße

Wir sehen die gleiche Tendenz wie bei den Durchschnittswerten des Funnels auf Seite 16. Die größte Veränderung im Vergleich zum vorherigen Bericht ist bei großen Organisationen zu beobachten, die im vergangenen Jahr mit umfangreichen Mengen an Malware zu kämpfen hatten. In diesem Jahr standen bei allen Unternehmensgrößen Network & Application Anomalies an erster Stelle der Incident-Typen.

Zwei Faktoren fallen jedoch auf: Kleine Organisationen leiden sehr viel stärker unter Kontoanomalien (29% im Vergleich zu 24% bei mittleren und 17% bei großen) und große Organisationen müssen immer noch mehr als doppelt so viele Malware-Angriffe abwehren wie kleinere.

Im Durchschnitt ist die Zahl der Vorfälle pro Kopf in kleinen Unternehmen etwa vierzehnmal höher als in großen Organisationen. Dies bestätigt einen Trend, den wir auch in früheren Berichten beobachtet haben. In unserem letzten aktualisierten Bericht stellten wir fest, dass dieser Faktor sechsmal so hoch ist. Mit der Verdoppelung des Faktors für 2019 sehen wir, dass diese Tendenz rasch an Fahrt gewinnt.



Incidents
Pro 100 Mitarbeiter

Bei Organisationen mit weniger als 1.000 Mitarbeitern beobachteten wir erneut einen starken Anstieg der Incident Quote. Im Durchschnitt ist die Zahl der Vorfälle pro Kopf etwa vierzehnmal höher als in großen Organisationen.

Mittlerweile ist fast jede dritte Person, die in einer kleineren Organisation arbeitet, direkt von einer Cyber-Bedrohung betroffen.

Small Organizations	Medium Organizations	Large Organizations
29.5	6.4	2.1

Kritikalität

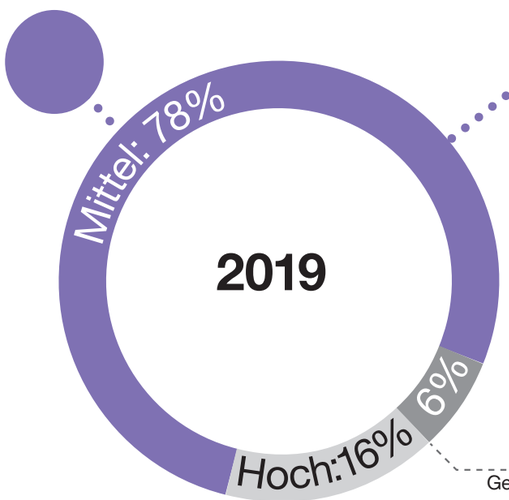
Incidents sind nicht immer gleich. Bei Orange Cyberdefense haben wir vier Stufen definiert:

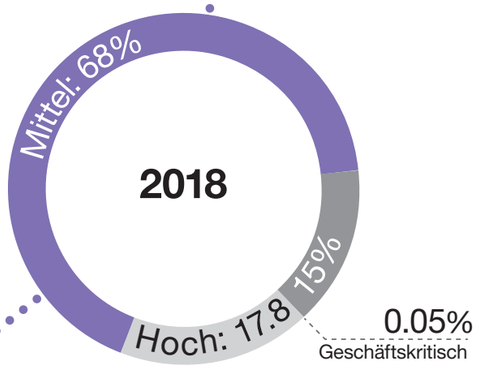
- **Geschäftskritisch:** Kritische Geschäftsauswirkungen, Geschäftsprozesse kommen zum Erliegen
- **Hoch:** Erhebliche geschäftliche Auswirkungen, Vorfälle, die sofort behandelt werden müssen
- **Mittel:** Begrenzte Auswirkungen auf das Geschäft, akzeptable Workarounds könnten vorhanden sein
- **Niedrig:** Minimale Auswirkungen auf das Geschäft, hat keine signifikanten Auswirkungen auf den Betrieb

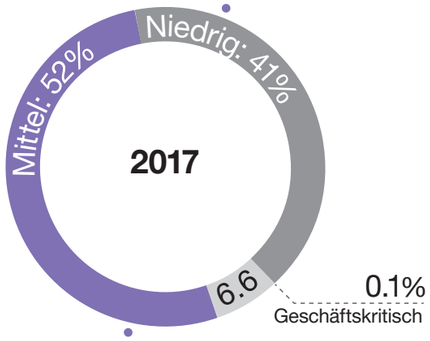
	Geschäfts-kritisch	Hoch	Mittel	Niedrig
2016	0.50%	8.2%	53%	38%
2017	0.10%	6.6%	52%	41%
2018	0.05%	17.8%	68%	15%
2019	0.11%	16%	76%	7%

Im Jahr 2019 sehen wir, dass sich zwei Trends aus den beiden Vorjahren fortsetzen: Zwischenfälle der mittleren Kategorie haben im Vergleich zum Vorjahr erneut um fast 10% zugenommen. In der Zwischenzeit haben sich die Vorfälle mit niedriger kritischer Bewertung etwa halbiert, was erneut darauf hindeutet, dass das "Grundrauschen" der einfallslosen Massenangriffe schnell an Boden verliert gegenüber einem zunehmenden Niveau der Security.

Die als hoch eingestuften Angriffe sind mit 16,04% stagnierend geblieben. Von 2017 bis 2018 haben sich diese verdreifacht, so dass es eine Erleichterung ist, dass dies nicht mehr vorkam. Was jedoch ein unbehagliches Gefühl hinterlässt, ist die Tatsache, dass die Zahl der als geschäftskritisch eingestuften Angriffe zwar mit 0,11% nicht dramatisch hoch ist, sich aber dennoch im Vergleich zu 2018 verdoppelt hat. Dies ist vergleichbar mit dem Status von 2017.







Operation “Sharpshooter” North Korea zugeschrieben

Die weltweite Spionagekampagne zielte auf kritische Infrastrukturen wie Regierungsinstitutionen, Kraftwerke und Finanzorganisationen ab. Potenzielle falsche Flaggen erschwerten die Zuschreibung, aber jetzt haben Forscher von McAfee die Kampagne offiziell der vom nordkoreanischen Staat gesponserten Lazarus-Gruppe zugeschrieben [t12].

Mozilla führt Firefox Send ein, einen kostenlosen verschlüsselten Dateiübertragungsdienst

Es erlaubt Benutzern, Dateien von bis zu 1 GB hochzuladen (bis zu 2,5 GB für registrierte Benutzer) und den Download-Link freizugeben [t13].

MÄR

Runde 4 - Hacker stellt 26 Millionen neue Konten im Darkweb zum Verkauf

"Gnosticplayers" schlägt wieder zu: 26 Millionen neue Datensätze zum Verkauf [t14].

Mirai ist zurück

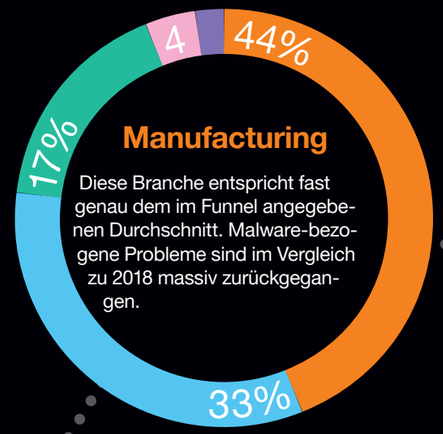
Das IoT-Botnet Mirai taucht als "Enterprise Edition" wieder auf und zielt nun speziell darauf ab, intelligente Unternehmensgeräte wie drahtlose Präsentationssysteme und Router in DDoS-Bots zu verwandeln [t15].

Incidents in verschiedenen Bracnhen

Wie sind die Vorfälle innerhalb der verschiedenen Branchen verteilt? Wir analysierten sieben Branchen und waren überrascht über die Unterschiede, die wir entdeckten.

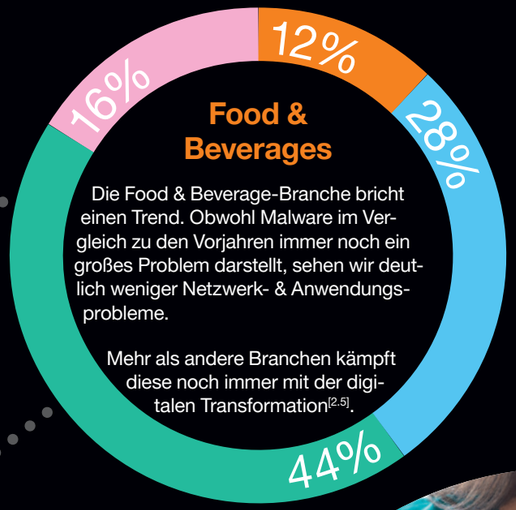
Höhere Prozentsätze in diesen Diagrammen bedeuten nicht nur, dass Vorfälle häufiger vorkommen und dass die Branche "anfälliger" ist. Sie können sogar das genaue Gegenteil anzeigen. Die Fähigkeit, einen Vorfall zu identifizieren, kann auf eine hohe Sicherheitsreife hindeuten. Zum Beispiel gibt es im Finanzwesen ein hohes Maß an Social Engineering für Betrugszwecke, weil die Finanzorganisationen im Umgang mit diesen Vorfällen reifer sind und mehr von ihnen erkennen und melden können.

	Network	Account	Malware	System	Policy	Social
Professional Services	59.93%	22.68%	10.85%	5.50%	0.94%	0.10%
Financial Services	45.06%	26.48%	11.76%	6.19%	0.11%	10.41%
Manufacturing	44.38%	32.63%	16.94%	4.39%	1.63%	0.03%
Food & Beverages	12.13%	27.62%	43.51%	16.32%	0.00%	0.42%
Government&Public	49.17%	41.72%	5.30%	1.16%	2.65%	0.00%
Healthcare	83.19%	5.75%	9.02%	1.84%	0.03%	0.19%
Education	39.25%	57.01%	0.47%	0.00%	2.80%	0.47%
Biotechnology	42.37%	49.57%	4.76%	3.30%	0.00%	0.00%
Retail	34.33%	18.49%	27.84%	12.11%	5.77%	1.46%



Manufacturing

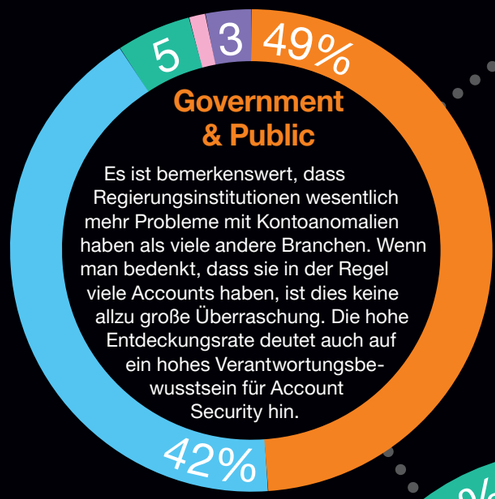
Diese Branche entspricht fast genau dem im Funnel angegebenen Durchschnitt. Malware-bezogene Probleme sind im Vergleich zu 2018 massiv zurückgegangen.



Food & Beverages

Die Food & Beverage-Branche bricht einen Trend. Obwohl Malware im Vergleich zu den Vorjahren immer noch ein großes Problem darstellt, sehen wir deutlich weniger Netzwerk- & Anwendungsprobleme.

Mehr als andere Branchen kämpft diese noch immer mit der digitalen Transformation[2.5].



Government & Public

Es ist bemerkenswert, dass Regierungsinstitutionen wesentlich mehr Probleme mit Kontoanomalien haben als viele andere Branchen. Wenn man bedenkt, dass sie in der Regel viele Accounts haben, ist dies keine allzu große Überraschung. Die hohe Entdeckungsrate deutet auch auf ein hohes Verantwortungsbewusstsein für Account Security hin.

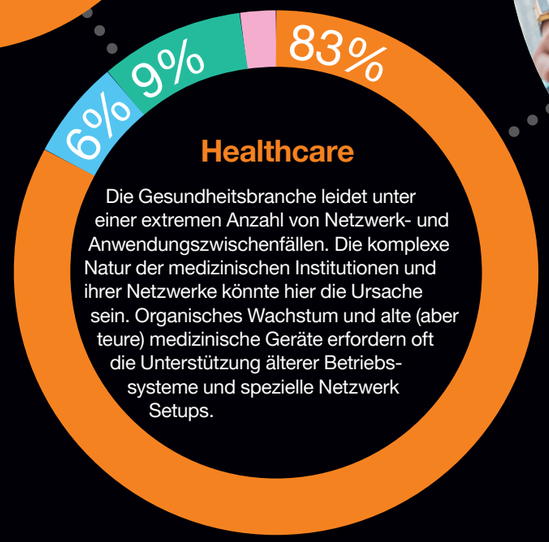
Professional Services

Wir stellen fest, dass diese Branche eng mit dem Profil übereinstimmt, das bei Organisationen mit bis zu 1.000 Beschäftigten beobachtet wurde.

Financial Services

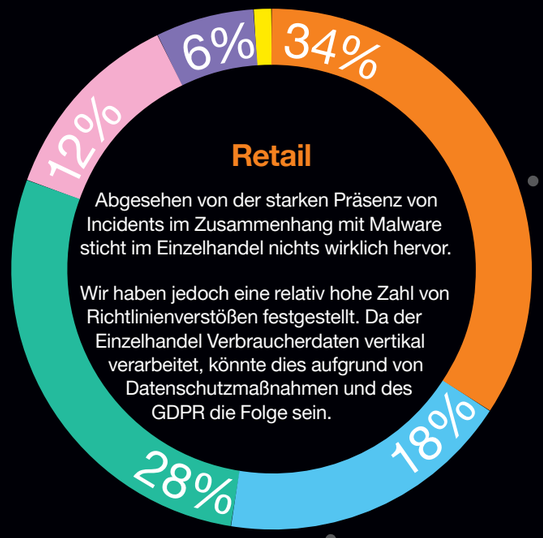
Der bemerkenswerteste Aspekt der Finanzbranche ist ihre hohe Sensibilität für Social Engineering.

Dies ist wahrscheinlich auf eine Kombination aus dem exzessiven Einsatz von Social-Engineering-Taktiken zur Untergrabung ihrer traditionell starken Cyber-Sicherheit sowie auf eine Wirkung der daraus resultierenden Detection-Fähigkeiten zurückzuführen, die ausgereifter sind als in jeder anderen Branchen.



Healthcare

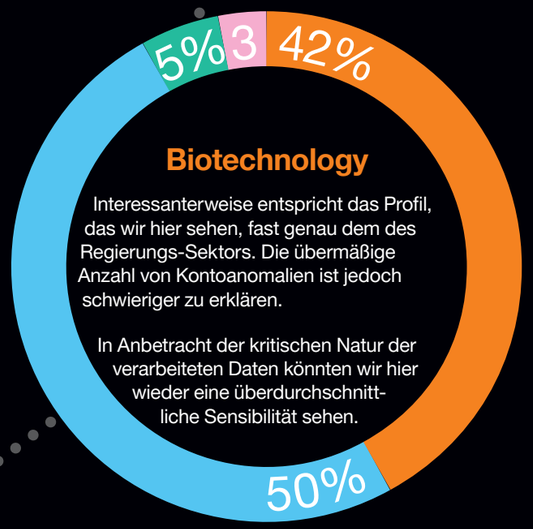
Die Gesundheitsbranche leidet unter einer extremen Anzahl von Netzwerk- und Anwendungszwischenfällen. Die komplexe Natur der medizinischen Institutionen und ihrer Netzwerke könnte hier die Ursache sein. Organisches Wachstum und alte (aber teure) medizinische Geräte erfordern oft die Unterstützung älterer Betriebssysteme und spezielle Netzwerk Setups.



Retail

Abgesehen von der starken Präsenz von Incidents im Zusammenhang mit Malware sticht im Einzelhandel nichts wirklich hervor.

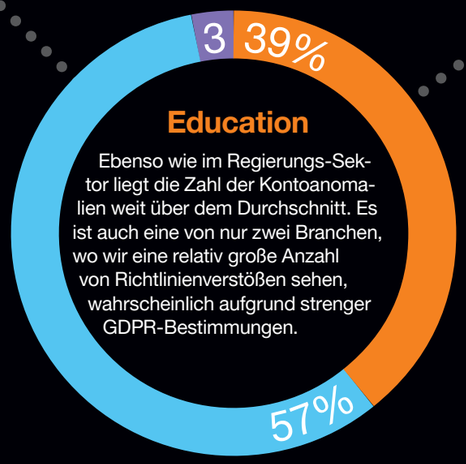
Wir haben jedoch eine relativ hohe Zahl von Richtlinienverstößen festgestellt. Da der Einzelhandel Verbraucherdaten vertikal verarbeitet, könnte dies aufgrund von Datenschutzmaßnahmen und des GDPR die Folge sein.



Biotechnology

Interessanterweise entspricht das Profil, das wir hier sehen, fast genau dem des Regierungs-Sektors. Die übermäßige Anzahl von Kontoanomalien ist jedoch schwieriger zu erklären.

In Anbetracht der kritischen Natur der verarbeiteten Daten könnten wir hier wieder eine überdurchschnittliche Sensibilität sehen.



Education

Ebenso wie im Regierungs-Sektor liegt die Zahl der Kontoanomalien weit über dem Durchschnitt. Es ist auch eine von nur zwei Branchen, wo wir eine relativ große Anzahl von Richtlinienverstößen sehen, wahrscheinlich aufgrund strenger GDPR-Bestimmungen.

Fazit

Die Spannung hat zugenommen. Betrachtet man das Verhältnis zwischen den gesamten Alerts und sicherheitsrelevanten Incidents, so sehen wir eine Tendenz zur Verschlechterung. Diese Veränderung ist zum Teil auf die kontinuierliche Arbeit zurückzuführen, die in die Feinabstimmung der Warnungen investiert wurde (Beseitigung von Fehlalarmen), aber sie zeigt auch, dass uns die Bedrohungsakteure immer noch auf den Fersen sind.

Im vorherigen Bericht war die Hauptquelle von Incidents Malware, die fast die Hälfte der Angriffe ausmachte, die wir in unseren CyberSOCs entdeckt hatten. In diesem Jahr ziehen netzwerkbezogene Vorfälle an die Spitze.

Die Reduzierung von Malware wurde dank der Implementierung der neuesten Generation von Endpoint Protection durch viele unserer Kunden erreicht.

Nichtsdestotrotz sollten Kontoanomalien und Malware nicht unterschätzt werden. Sie sind nach wie vor relevante potenzielle Bedrohungen mit erheblichen Auswirkungen auf die Opfer, wenn sie getroffen werden. Endpoint Detection and Response könnten dazu beitragen, das Risiko weiter zu reduzieren, da ab einem bestimmten Punkt die Erkennung bessere (und kosteneffizientere) Ergebnisse liefert als übermäßige Ausgaben für die Prävention allein. Darüber hinaus ergänzen die Network Traffic Detect and Respond-Technologien die Endpoint- und SIEM-basierte Detektion.

Eine beträchtliche Verschiebung der Angriffe, die auf kleine und mittlere Organisationen abzielen, deutet eindeutig darauf hin, dass der Mittelstand seine Sensibilität für Cybersecurity-Bedrohungen besser erhöhen sollte.

Diese Investitionen sind nicht auf Technologie beschränkt: Der Zugang zu Experten mit den richtigen Fähigkeiten ist von wesentlicher Bedeutung. Und in einem Markt, in dem Cyber-Expertise rar ist - laut dem gemeinnützigen ISC2 sind heute bis zu 2,9 Millionen offene Stellen zu besetzen – kommt Managed Detection and Response immer mehr in den Fokus. Große Unternehmen und multinationale Konzerne haben sich früh angepasst, und wir nehmen an, dass auch das Interesse mittelständischer Unternehmen rasch zunimmt.

Im nächsten Security Navigator im Dezember wird es sehr interessant zu sehen, wie sich die Zahlen aufgrund der massiven Auswirkungen der COVID-19-Krise verändert haben. Sowohl die Bewegung in Richtung Homeoffice während des Lockdowns als auch die veränderten Angriffsmuster innerhalb der Angreifer-Community könnten eine bedeutende Wirkung haben.

Norsk Hydro legt globales Netzwerk nach Ransomware-Attacke lahm

Mehrere Anlagen in verschiedenen Ländern mussten aufgrund einer Infektion mit LockerGoga, die sich von den US-Standorten aus ausbreitete, abgeschaltet oder im manuellen Modus betrieben werden [t16].

APR

Implantierte Defibrillatoren anfällig für Hacking

Die von Medtronic hergestellten Geräte arbeiten mit einem proprietären funkbasierten Verbindungsprotokoll, dessen Implementierung grundlegend fehlerhaft ist: Es enthält keinerlei Verschlüsselung, Authentifizierungsprüfungen oder Datenvalidierung [t17].

Bithumb (erneut) gehackt: 19 Millionen Dollar gestohlen

3 Millionen EOS und 20 Millionen XRP wurden aus kompromittierten Wallets gestohlen. Erst letztes Jahr hatte Bithumb bereits EOS im Wert von 32 Millionen Dollar verloren, die aus den Wallets vieler seiner Benutzer gestohlen wurden [t18].

540 Millionen Facebook-Benutzer-Datensätze auf ungeschützten Amazon-Servern gefunden

Das mexikanische Medienunternehmen Cultura Colectiva hatte 146 GB an Daten mit Kommentaren, Vorlieben, Kontonamen und Benutzer-IDs von Facebook gesammelt und auf den Servern von AWS öffentlich zugänglich gemacht. Offenbar hat Facebook bereits die Kontrolle über die Daten von Millionen von Nutzern an Dritte verloren [t19].

Neues APT-Framework namens "TajMahal" entdeckt

TajMahal ist ein Toolkit mit einem erstaunlichen Set von 80 Modulen und enthält Tricks, die "noch nie zuvor gesehen" wurden. Es existiert anscheinend seit mindestens fünf Jahren, wurde aber bisher noch nie entdeckt [t21].

Chat der französischen Regierung "Tchap" gehackt

Aufgrund einer unsachgemäßen Validierung der erlaubten E-Mail-Adressen konnte sich der französische Sicherheitsforscher Elliot Alderson in die App einloggen, die auf Regierungsbeamte hätte beschränkt werden müssen [t22].

Electrum Wallet Infection breitet sich rasch aus und stiehlt 4,6 Millionen Dollar

Der Angriff bestand aus einer Reihe von gehackten Servern, die vorgaben, Teil des Electrum-Peer-Netzwerks zu sein. Diese antworteten mit einer gefälschten Fehlermeldung auf legitime Anfragen, indem sie die Electrum Wallet-Apps austricksten, um ein böswilliges Update herunterzuladen, das dann Gelder aus dem Wallet stahl und zusätzlich eine Botnet-Infektion enthielt, die zum DDoS legitimer Electrum-Server verwendet wurde [t23].

MAI

Fleury Michon stellt wegen eines Computervirus die Produktion für fünf Tage ein

11 Produktionsstätten sowie die Logistikabteilung wurden stillgelegt.

Das Management behauptet, dass die Kosten des Ausfalls durch eine Cyberversicherung gedeckt sind [t24].

Mysteriöse Datenbank mit Daten von 80 Millionen US-Bürgern gefunden

Die bekannten Hacktivisten Noam Rotem und Ran Locar entdeckten eine ungeschützte Datenbank mit Informationen mit bis zu 65 % der US-Haushalte, die auf einem Cloud-Server von Microsoft gehostet wird. Es ist noch unbekannt, wem diese Datenbank gehört oder welchem Zweck sie dient [t25].

Stadt Baltimore durch Ransomware lahmgelegt

Während Notrufleitungen wie die 911 nicht betroffen waren, gab es bei den meisten öffentlichen Diensten wie den Abteilungen für öffentliche Arbeiten, Finanzen und Verkehr Ausfälle von E-Mail- und Telefonleitungen [t27].

Europol schaltet Wall Street Market und Silkkitie (alias Valhalla) ab

Internationale Strafverfolgungsbehörden haben zwei berüchtigte Verkaufsplatt-formen im Darknet aufgedeckt. Der Wall Street Market war einst die zweitgrößte Plattform weltweit mit etwa 5400 Anbietern und Millionen von Nutzern, die mit Waren wie Drogen, gestohlenen Daten, Hackerdiensten und Malware-Code handelten [t26].

Website der Aéroports de Lyon im Visier eines Cyber-Angriffs

Kunden, die auf der Homepage des Flughafens Dienstleistungen wie Parkplätze und Lounges buchen, wurden auf eine Phishing-Website umgeleitet, auf der versucht wurde, ihre Anmeldedaten und Daten zu stehlen [t28].

Paul van der Haas
Lead Engineer Operations SLI
Orange Cyberdefense

Thomas Eeles
CSIRT Manager
Orange Cyberdefense

Pentesting & CSIRT Stories

Geschichten aus dem Low-Level

Es war einmal ein Pentest

Im Laufe der Zeit haben die Pentester einen gewissen Ruf und ganz besondere Fähigkeiten erworben. Diese Fähigkeiten unterscheiden sich nicht allzu sehr von den Bösewichten, die die Organisationen so verzweifelt in Schach halten wollen; obwohl man uns zutraut, unsere Ergebnisse auf verantwortungsvolle Weise offenzulegen. Aber wir trinken Kaffee, und zwar viel davon, und genießen Donuts. Die mit Zuckerstreuseln!

Reputation ist gleich Vertrauen. Kunden lernen uns kennen, sie bewundern unsere Fähigkeiten und bauen Vertrauen zu uns auf, und sie laden uns dazu ein, ihre Schwächen aufzuspüren und auszunutzen. Wie lässt sich das wahre Cyberrisiko besser demonstrieren?

Unser Ruf eilt uns voraus. Unser eigenes Sales-Team rühmte sich oft unserer Fähigkeiten: Wir freuten uns über die kurze Zeit, die es dauern würde, ein Domainadministrator-Konto einzurichten, und das alles, bevor der erste Kaffee fertig war und der Kunde mit den gestreuselten Donuts zurückgekehrt war.

Die Zeiten haben sich geändert, Geschichten wie diese sind Cyber-Geschichte. Bald werden solche Märchen in Fabeln erscheinen, und die Gute-Nacht-Geschichten unserer Kinder werden die Pentester von einst populär machen. Also schnappen Sie sich die Marshmallows und folgen Sie uns auf das Low-Level!

Story 1: (Un-)Sicherheit voreingestellt

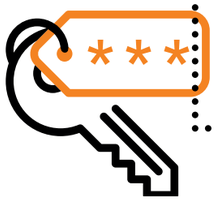
Ein neuer Auftrag kam von einem Kunden mit folgenden spezifischen Zielen: Identifizierung von Schwachstellen im internen Netzwerk und weitere Ausnutzung und Durchdringung des Netzwerks. Ein typischer Auftrag mit der Erlaubnis auszunutzen und zu erforschen; etwas, das wir sehr gut machen.

Der Kaffee kam an, und mit ihm die Donuts, und wir machten uns daran, das Kundennetzwerk mit Scan-Software zu entdecken.

1 Scan

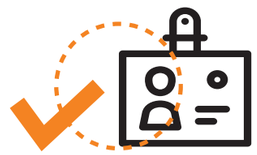
Der Kaffee war noch warm, die Scans liefen noch, und ein Mitglied unseres Teams erklärte, er habe bereits eine Webanwendung entdeckt, die wie ein Verwaltungsportal für das Active Directory des Kunden aussah.

Wenn man sich an vergangene Zeiten erinnert, sollte es doch nicht möglich sein, sich mit admin/admin einzuloggen, oder?



2 Anmeldung mit Standard-Login

Trinken Sie Ihren Kaffee aus, packen Sie den Laptop weg, ein neuer Domain-Administrator ist im Haus!



3 Privilegierten Zugang erlangen

Wie Sie vielleicht schon vermutet haben, war es möglich, sich mit diesen Zugangsdaten anzumelden. Die Anwendung verwendete ein Konto mit privilegiertem Zugriff auf das Active Directory des Kunden.

Entwickelt, um die Verwaltung der Domäne zu erleichtern, ermöglicht es Helpdesk-Administratoren die Verwaltung von Benutzerkonten.

4 Verschleierung ist keine Sicherheit

Mit guten Absichten hatte der Kunde das Domainadministrator-Konto dafür konfiguriert. Der Anwendungsfall versteckte das Passwort des Kontos mit einer grundlegenden Verschleierung, aber nur auf der Client-Seite.

5 Die Schwächen ausnutzen

Unter Ausnutzung der clientseitigen Schwäche war es möglich, das Kennwortfeld so zu ändern, dass das Kennwort im Klartext angezeigt wird, was dem Pentester im Wesentlichen die Anmeldedaten des Domainadministrators offenbart.

6 Vollständig kompromittiert

Das privilegierteste Konto in der IT war erfolgreich gekapert, obwohl noch mehr als die Hälfte der Donuts übrig war.

Die Fahne wurde erobert, die Ziellinie war überquert, alles, was der Kunde für sicher gehalten hatte, galt nun als kompromittiert.

JUN

GoldBrute hat es auf 1.5 Millionen RDP-Server abgesehen

Die laufende Botnet-Kampagne zielt darauf ab, Anmeldungen auf geöffneten Windows RDP-Server per brute-force zu erzwingen. Um eine Erkennung zu vermeiden, sendet jeder Bot nur einen Loginversuch an viele verschiedene Server, sodass jede Anforderung von einer anderen IP stammt [t29].

Lessons learned

Obwohl dieses Pentest-Kapitel nur ein kurzer Auszug aus der IT-Geschichte eines Kunden ist, können sicherlich viele Lektionen daraus gezogen werden. Was ist bei diesem Kunden wirklich schiefgelaufen? Waren es die Standard-Anmeldeinformationen, oder war die Anwendung nicht in der Lage, die Credentials des Domainadministrators ausreichend zu schützen?

Wir müssen ein wenig weiter zurückgehen, um das zu verstehen. Die IT-Security räumt ein, dass Sicherheitskontrollen versagen werden, daher ist es einfach nicht effektiv, sich auf eine einzige Kontrolle zu verlassen. Verfolgt man die Geschichte von Anfang an, so wird man schwache oder sogar fehlende Kontrollen feststellen:

- **Network Access Controls (NAC):** Die Tester konnten sich ohne jede Herausforderung an das Netzwerk anschließen. NAC hätte dem Pentester die Arbeit erschweren können, sich einfach an das Netzwerk und seine Dienste anzuschließen.
- **Principle of Least Privilege:** Übermäßig freizügige Credentials. Das Domänenadministratorkonto hat einen Zweck: die Verwaltung der Domain (vom Domaincontroller aus). Der Zugriff auf dieses Konto sollte extrem eingeschränkt sein.
- **Segmentation and Filtering:** Die gefundene Anwendung wurde zur Verwaltung von Benutzerkonten verwendet. Es gab keinen Grund dafür, dass ein nicht-administratives Gerät auf die Anwendung zugreift. Eine funktionale Segmentierung sollte vorhanden sein und zugelassenen Zugriff auf die Anwendung filtern. Denken Sie immer an das Prinzip der geringsten Privilegien!
- **Standard-Anmeldeinformationen:** Ändern Sie immer die Standard-Anmeldedaten des Systems und der Anwendung. Die Standard-Logins sind absichtlich schwach und oft öffentlich bekannt. Es sollten Richtlinien und Verfahren festgelegt werden, die eine Änderung der Standard-Credentials erfordern.

CSIRT Stories

In diesem Jahr hat das CSIRT bei Orange Cyberdefense noch nie dagewesene Vorfälle im Bereich der Cybersecurity bewältigt. Ein stetiger Strom von Microsoft Office 365 E-Mail-Hacks wurde für groß angelegte Ransomware-Attacken missbraucht. Keiner von ihnen war ein "nationalstaatlicher Angriff", und die Mehrheit war nicht das, was wir als übermäßig raffiniert einstufen würden. Sie haben jedoch alle schweren Schaden angerichtet, bevor wir hinzugezogen wurden. In diesem Abschnitt werden wir uns mit einer kleinen Auswahl einiger der Fehler befassen, die wir 2019 erlebt haben, und mit dem Schaden, den sie angerichtet haben.

Story 2: Die millionenschwere Datenpanne

Das ist der Stoff, aus dem IT-Alpträume sind. Die Fabel so alt wie die IT: "Niemand wird uns hacken, wir haben nichts, was sich zu stehlen lohnt". Warum sich also die Mühe machen, die grundlegendsten Best Practices der Branche anzuwenden?

Das ist genau das, was wir gefunden haben. Ein völlig flaches Netzwerk, ohne Backups, über 30 Domänenadministratorkonten und ohne zentrale Protokollierung.

1 Das Word-Makro aus der Hölle

Letzteres bedeutete, dass, wenn jemand ein mit einem Makro präpariertes Word-Dokument öffnete, niemand bemerkte, dass das Antivirenprogramm einen Download von Emotet festgestellt (aber nicht blockiert) hatte. Auch hat niemand bemerkt, dass kurz danach ein lokales Admin-Konto zur Installation einiger Netzwerkanalysetools verwendet wurde.

2 Ohne Vorwarnung

Ein gutes Security Operations Centre (SOC) hätte bei jedem dieser Vorfälle eine Frühwarnung ausgeben können. Es hätte alles bereinigt werden können und der Endnutzer hätte eine Schulung erhalten können, um zu verhindern, dass sich solche Vorfälle wiederholen.

Aber das ist nicht passiert.

3 Jackpot für Hacker

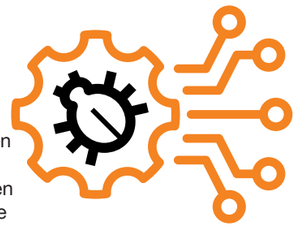
Die Angreifer hatten Glück: Der Schutz des lokalen Admin-Kontos auf dem Endpoint, auf den sie Zugriff hatten, war, um höflich zu sein, sehr schwach.

Als wäre das nicht schon beunruhigend genug, kommt noch dazu, dass das lokale Administrator-Passwort auf jedem Endpoint des Netzwerks, einschließlich Server und Hypervisor, dasselbe war.

Dadurch hatten die Angreifer uneingeschränkten Zugang zum gesamten Netzwerk, ohne dass jemand beobachtete, was sie gerade taten.

4 Lateral Movement & Zerstörung

Also legten die Angreifer los: Löschen von Backups, Deaktivieren von AV, Erstellen von Domain-Administrator-Accounts, Verwenden von Blood Hound, um das gesamte Netzwerk abzubilden, und Öffnen von Firewalls für Remote Desktop (RDP)-Verbindungen nach außen.



5 Ransomware installiert

Der Angriff erreichte einen verheerenden Höhepunkt, als die allseits beliebte Ryuk-Ransomware in einem versteckten Freigabeordner auf dem Domänencontroller des Kunden abgelegt wurde. Zusammen mit einer Liste von über 4.000 Microsoft Windows-Endpoints in einer einfachen ".txt"-Datei, einer einzelnen ".bat"-Datei und einer Kopie der legitimen Windows-"PsExec"-Binärdatei.

Mit einem Klick hat die bat-Datei Ryuk auf das Netzwerk losgelassen, wobei jede nutzbare Datei verschlüsselt und das Geschäft zum völligen Stillstand gebracht wurde.

6 Recovery

Insgesamt arbeitete das Orange Cyberdefense CSIRT vier Wochen lang daran, das Netzwerk wieder zum Laufen zu bringen.

Entgegen aller Ratschläge von Orange Cyberdefense zahlte der Kunde eine halbe Million Euro an die Angreifer, um Entschlüsselungsschlüssel zu erhalten. Dazu kam noch, dass sie einer Anwaltskanzlei Hunderttausende von Gebühren zahlen mussten, um die Zahlung abzuwickeln (was die Frage aufwirft, wer die wirklichen Kriminellen hierbei sind), und weit über eine halbe Million mehr an Netzwerk-Upgrades und Richtlinienänderungen, um das beschädigte Netzwerk in einen sauberen und vertrauenswürdigen Zustand zu bringen.

GandCrab-Verschlüsselung geknackt

Ein kostenloses Entschlüsselungsprogramm für die Anfang des Jahres entdeckte GandCrab Ransomware wurde veröffentlicht [t30].

Lessons learned

Was sollten Sie also aus dieser Horror-Story mitnehmen?

Die meisten Schwachstellen im Netzwerk hätten leicht ausgebessert werden können: Die Netzwerksegmentierung ist wahrscheinlich die grundlegendste aller Sicherheitsmaßnahmen, ebenso wie starke Passwortrichtlinien und Einschränkungen der Benutzerrechte. Diese Maßnahmen wirken sich in gewissem Maße auf die Arbeitsweise des IT-Personals aus, sind aber nicht sehr kostspielig in der Umsetzung. Zugegebenermaßen ist die Nachrüstung eines SOC ein großes Projekt, aber gerade deshalb sollten Sie sicherstellen, dass Ihr Netzwerk von Anfang an bewährte Verfahren implementiert.

Der erschreckendste Teil dieser Geschichte: Wir haben viele Details aus Gründen des Datenschutzes ausgelassen.

In Wirklichkeit war es viel schlimmer.

Story 3: Eine delikate E-Mail-Affäre

Obwohl dieser Angriff den CFO des Kunden nicht so sehr beunruhigte wie die erste Geschichte, hielt sie das PR-Team nachts wach und beunruhigte es einige Wochen lang. Es ist nichts Neues, dass jetzt mehr Unternehmen auf die Cloud vertrauen. Besonders, wenn es um E-Mails und Dateifreigaben geht, wobei Microsoft Office 365 (O365) den Löwenanteil des E-Mail-Hostings für große Unternehmen übernimmt.

Wie bei vielen anderen IT-Bereichen hat diese Verschiebung in der Praxis zu einigen Security-Schnitzern geführt.

1 High-Level Spam

Anfang 2019 kontaktierte uns ein Kunde mit einer "sensiblen" Angelegenheit im Zusammenhang mit einem O365-E-Mail-Hack.

Um das PG-Rating dieses Berichts beizubehalten, möchte ich nur sagen, dass Spam-E-Mails eher erwachsener Natur an Hunderttausende von Konten von dem Account einer hochrangigen Person in der Organisation aus herumgeschickt worden waren.

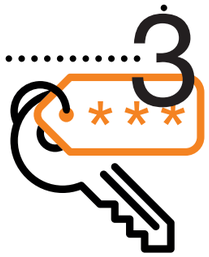
2 Schlechte PR ist nicht das einzige Problem

Dies warf zwei Probleme für den Kunden auf; das offensichtlichste ist der Public-Relations-Alptraum: Ein Vorstandsmitglied einer Organisation, spamt so viele Menschen mit völligem Unsinn zu.

Zweitens: Jemand hatte potenziell Zugang zu hochsensiblen E-Mails in der O365-Umgebung des Kunden.

Haben die Angreifer Kopien kritischer E-Mails weitergeleitet oder heruntergeladen?

Es wurde schnell klar, dass der fragliche Benutzer Ziel eines Passwort-Stuffing-Angriffs war.



3 Password Stuffing

Wie sich herausstellte, war der Angriff weit größer als zunächst angenommen.

Tausende von Benutzernamen- und Passwort-Kombinationen waren auf die O365-Infrastruktur der Organisation gerichtet worden. Anhand von Protokollen, die wir von Microsoft erhielten, konnten wir herausfinden, dass die verwendete Liste wahrscheinlich die LinkedIn-Passwortdatenbank aus dem Jahr 2016 war. Der Benutzer des ersten gehackten Kontos hatte sowohl für LinkedIn als auch für sein Firmen-E-Mail-Konto die gleiche E-Mail- und Passwort-Kombination.

4 Verbot von unsicheren Passwörtern

Wir stellten fest, dass weit über hundert Konten von vier verdächtig aussehenden IP-Adressen aus aufgerufen wurden, die wir mit ähnlichen "Schmuddel"-Spamming-Kampagnen in Verbindung bringen konnten.

Dies ist die erste Stufe, in der der Kunde Schutzvorkehrungen hätte treffen können, um das Risiko zu mindern. Benutzer an der Wiederverwendung von Passwörtern zu hindern, ist schwierig, aber nicht unmöglich. Bekannte durchgesickerte Passwörter können für die Verwendung in Unternehmensnetzwerken gesperrt werden, Dienste wie "Have I Been Been Pwned" ermöglichen es, Passwort-Hashes mit bekannten Listen abzugleichen.

5 Zurückverfolgen des Angriffsverlaufs

Sobald wir alle Konten identifiziert hatten, die während des Angriffs "aufgeflogen" waren, begannen wir damit, herauszufinden, was passiert war, und welchen Zugang zu Daten die Angreifer möglicherweise hatten.

6 Automatisiertes Hacking, aber kein Datenleck

Anhand von Zeitstempeln war erkennbar, dass der Angriff automatisiert war. Die Zeitverzögerung vom Zeitpunkt des Zugriffs bis zum Zeitpunkt der ersten versandten E-Mails betrug nur wenige Sekunden, und das Volumen der in einem so kurzen Zeitrahmen versandten E-Mails passte zu anderen Kampagnen, die nachweislich automatisiert waren.

Wir haben auch keine Anzeichen dafür gefunden, dass E-Mails synchronisiert oder heruntergeladen wurden, noch gab es Weiterleitungsregeln für die betroffenen Konten.

7 Recovery

Alles, was wir sehen konnten, war, dass auf Hunderte von E-Mail-Konten zugegriffen wurde und dann Millionen von erstklassigen E-Mails verschickt wurden. Ein Download fand offenbar nicht statt.

Das machte den Datenschutzbeauftragten glücklich, tat aber wenig, um die Stimmung der PR- und Marketingteams zu verbessern.

Lessons learned

Wie bei der ersten Geschichte hätten einige einfache Änderungen an dem Setup das Ganze frühzeitig eindämmen können. Die Benutzer tendieren dazu, auf E-Mails von denselben Geräten und denselben IP-Adressen (zumindest vom IP-Block desselben Landes aus) zuzugreifen, daher ist die Warnung vor E-Mail-Zugriffen von anormalen IP-Adressen ein hervorragendes Instrument für Frühwarnungen. Insbesondere, wenn Sie dann diese IP-Adressen mit anderen Authentifizierungsversuchen korrelieren können.

Die einzige große Abhilfe ist jedoch die Zwei-Faktor-Authentifizierung (2FA). Im Jahr 2019 handelt jede Organisation, die über eine internetfähige Infrastruktur/Dienste verfügt, ohne 2FA riskant. 2FA stoppt die Mehrheit der "Drive-by"- oder "opportunistischen" Angriffe, die großen Schaden anrichten. Während das Scannen von IPs einfach und kostenlos durchgeführt werden kann, kann 2FA etwas schwieriger sein. Aber sehen Sie sich die Vorteile an, die sich aus dem Aufwand von ein oder zwei Wochen für die Einrichtung ergeben. Kein Zweifel, jeder sollte 2FA benutzen.

Da haben Sie es also, zwei Geschichten von der Pentesting- und CSIRT-Front, die Ihnen zeigen, was Sie tun sollten, um Finanz- und PR-Katastrophen zu verhindern. Wenn Sie sich einfach an die Best Practices der Branche halten würden, könnten viele Kunden das Risiko dieser spezifischen Angriffe drastisch reduzieren, und sobald Sie die Grundlagen beherrschen, können Sie sich damit befassen, wie man super gezielte Hacking-Versuche oder gar raffinierte nationalstaatliche Angriffe stoppen kann.

Facebook kündigt seine eigene Krypto-Währung "Libra" an

Gefolgt von sehr gemischten Reaktionen kündigte das mächtigste soziale Netzwerk der Welt an, im Jahr 2020 eine eigene Blockchain-basierte Krypto-Währung einzuführen [t31].

Laurent Célérier
EVP Technology & Marketing, Orange Cyberdefense
Ehemaliger Senior Officer, French Ministry Of Defense

Datenlecks überall:

Wo sind all die Daten geblieben?

Wenn man der Geschichte glauben darf, dann war 2017 ein herausragendes Jahr für Ransomware. Unsere armen Kollegen in der IT (und noch mehr unser CSIRT!) wachen des Nachts immer noch schweißgebadet auf aufgrund der Kampagnen von WannaCry, Petya und NotPetya.

Digitale Erpressung war nichts Neues, aber der Erfolg der Ransomware-Kampagnen 2017 war sicherlich berichtenswert. Beispiellose Medienaufmerksamkeit gepaart mit lahmgelegten Unternehmen. Es war ein Jahr, das wir nicht so schnell vergessen werden...

Das Jahr 2018 brachte eine neue Plage, die nicht ganz biblische Ausmaße hatte, aber Cryptomining hat sicherlich vielen digitalen IT-Geldbörsen (und Stromrechnungen) geschadet. Stark abhängig vom Wert von Bitcoin und anderen Krypto-Währungen, erlebten abtrünnige Miner in der ersten Hälfte des Jahres einen Boom und führten mehrere neue erfolgreiche Angriffsmethoden ein. Botnets hatten weltweit eine neue Mission, ihre Rechenkraft wurde von traditionellem Spamming und DDoS-Angriffen auf digitale Währungserzeugung umgestellt.

Doch was war die "große Sache" im Jahr 2019? Das Jahr ist vielleicht kein Olympisches Jahr, aber es wird als ein Jahr rekordverdächtiger Datenlecks in Erinnerung bleiben.

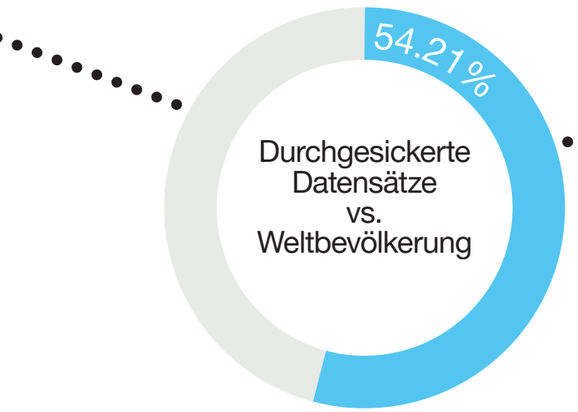
Timing ist alles

Bei der Verwaltung von Datenverstößen ist Zeit - und der Mangel daran - immer ein entscheidender Faktor. Viele Sicherheitsverletzungen werden erst Jahre nach ihrem ersten Auftreten entdeckt. Gelegentlich werden Datenschutzverletzungen sogar über mehrere Monate oder sogar Jahre hinweg begangen, bevor sie entdeckt werden. In den meisten Fällen werden Organisationen von Behörden oder Sicherheitsforschern, die Daten im Zusammenhang mit der Organisation in den dunkleren Teilen des Internets entdecken, über ihre Verletzung informiert; viel zu spät, um Schaden von den betroffenen Einzelpersonen und Organisationen abzuwenden. Es ist oft schwierig, zurückzuverfolgen und herauszufinden, wie und wann die Daten tatsächlich durchgesickert sind.

Milliarden sind betroffen

Im Jahr 2019 wurden 4.174.339.740 durchgesickerte Datensätze entdeckt. Bedenken Sie dies: Die Erdbevölkerung wurde im April dieses Jahres auf 7,7 Milliarden Menschen geschätzt[4.29], was bedeutet, dass möglicherweise von jedem zweiten Mensch personenbezogene Daten unrechtmäßig veröffentlicht wurden. Diese Zahl dürfte alarmierend sein, nicht nur für Datenschutzbegeisterte und Fans des GDPR.

Und das sind nur die Verstöße, von denen wir wissen.



Belagerte Unternehmen

Laut dem Midyear Data breach report[4.30] wurden in der ersten Hälfte des Jahres 2019 3.813 Datenverletzungen gemeldet, was einem Anstieg von fast 54% im Vergleich zur gleichen Zeit des Vorjahres entspricht. Im gleichen Zeitraum wurden acht Verstöße gemeldet, durch die über 100 Millionen Datensätze offengelegt wurden.

Mit 84,6% stammt die überwiegende Mehrheit davon aus dem Unternehmenssektor. Es überrascht auch nicht, dass Kriminelle in erster Linie E-Mail-Adressen suchen, die bei 70,5% der Verletzungen und Passwörter (64,2%) gefunden wurden[4.30]. Offensichtlich können gültige Anmeldeinformationen auf zahlreiche Arten missbraucht werden.

Die Methoden, mit denen Angreifer an große Datenmengen gelangen, sind nichts Neues: Taktiken wie Phishing und Skimming sind nach wie vor beliebt.

Statistisch war
jeder zweite
von einer Veröffentlichung
privater Daten
betroffen!

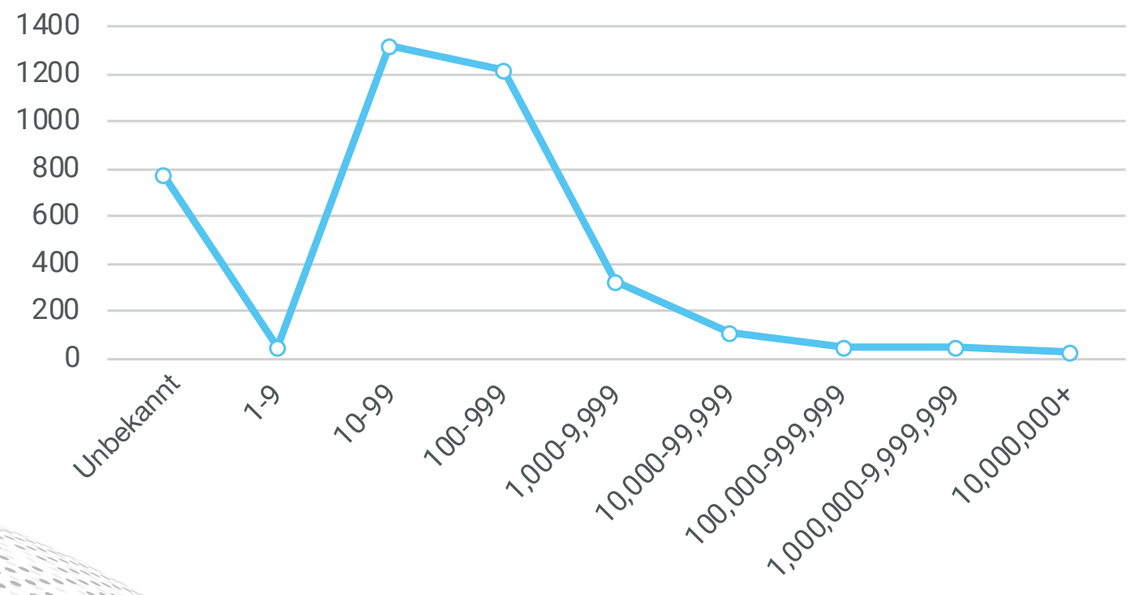
"Zu klein" gibt es nicht!

Die Medien nahmen die Gelegenheit wahr, die Verstöße größerer Organisationen aufsehenerregend darzustellen, und das zu Recht! Dies könnte den kleinen und mittleren Unternehmen den Druck nehmen. Es könnte jedoch auch zu einem falschen Gefühl der Sicherheit führen, insbesondere bei mittelständischen Organisationen. Wenn man die tatsächlichen Zahlen betrachtet, liegt hier ein gefährliches Missverständnis vor: Mehr als zwei Drittel der Daten wurden in kleinen Mengen von 1.000 Datensätzen oder weniger offengelegt. Es scheint, als ob alle Früchte für Kriminelle, unabhängig von ihrer Größe, gute Früchte sind.

Daten aus einem Verstoß treffen bald auf Daten aus einem anderen. Die Anreicherung von Daten schafft neue Möglichkeiten für Kriminelle und bietet ein nachhaltiges Geschäftsmodell für zuverlässige, qualitativ hochwertige Daten für diejenigen, die sie monetarisieren wollen.

Was später zum Verkauf angeboten wird, ist also oft eine Anhäufung von Tausenden von kleineren Unternehmen, die Datenverletzungen erlitten haben, oft ohne es zu wissen.

Verteilung nach Anzahl der gestohlenen Datensätze [4.30]



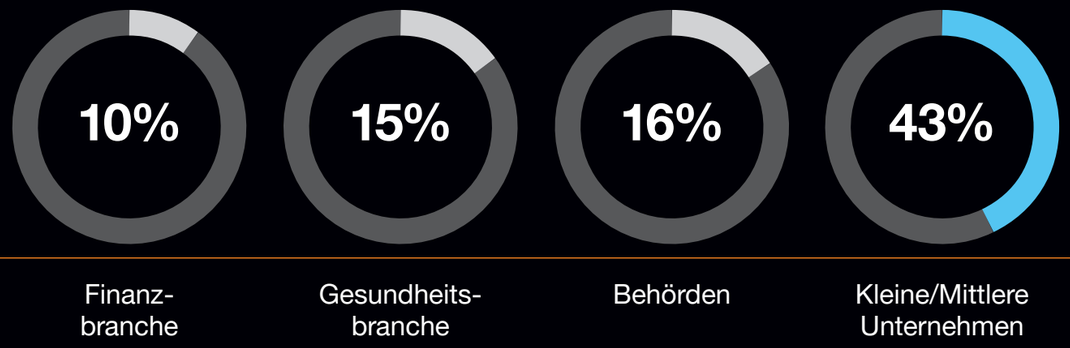
Warum auf den Baum klettern...

... wenn die Früchte vom Boden geerntet werden können?

Ok, auf dem Boden gefundene Früchte werden oft als ungenießbar angesehen, aber Daten enthalten keine Bakterien. Hacking monopolisiert immer noch die Statistik, wenn es um die Häufigkeit der Vorfälle (82%) geht, aber nicht, wenn es um die größte Menge an Aufzeichnungen geht. Tatsächlich sind die Zahlen irreführend. Wenn wir genauer hinsehen, stellen wir fest, dass 79% der tatsächlich offengelegten Daten wenig bis gar keinen Aufwand für die Harvester erforderten; wobei falsch konfigurierte Datenbanken, Webdienste und Anwendungen, oder über das Web zugängliche unsichere Cloud-Speicher zu den Beutezügen beitragen. Insider-Aktionen, sowohl böswillige als auch zufällige, sind eine weitere Hauptquelle.

Opfer von Datendiebstahl

Quelle: Verizon data breach report 2019[4.31]



Bemerkenswerte Datenlecks im Jahr 2019 (Januar-Oktober)

Breach	Datum	Anzahl Datensätze	Methode	Quelle
Collection 1	17. Jan	773.000.000	hacked	[4.1]
Universiti Teknologi MARA	25. Jan	1.164.540	hacked	[4.2]
Ministry of Health (Singapore)	28. Jan	14.200	schlechte Security/inside job	[4.3]
GnosticPlayers, Round 1	11. Feb	617.000.000	hacked	[4.4]
GnosticPlayers, Round 2	15. Feb	127.000.000	hacked	[4.5]
GnosticPlayers, Round 3	18. Feb	92.000.000	hacked	[4.6]
Health Sciences Authority (Singapore)	15. Mär	808.000	schlechte Security	[4.7]
GnosticPlayers, Round 4	17. Mär	26.000.000	hacked	[4.8]
Facebook	04. Apr	540.000.000	schlechte Security	[4.9]
Facebook	18. Apr	1.500.000	versehentlich hochgeladen	[4.10]
Justdial	18. Apr	100.000.000	ungeschützte api	[4.11]
Mystery Database	30. Apr	80.000.000	ungeschützt	[4.12]
Truecaller	22. Mai	299.055.000	unbekannt	[4.13]
First American Corporation	24. Mai	885.000.000	schlechte Security	[4.14]
Canva	28. Mai	140.000.000	hacked	[4.15]
Westpac	03. Jun	98.000	hacked	[4.16]
Australian National University	04. Jun	200.000	hacked	[4.17]
Quest Diagnostics	05. Jun	11.900.000	schlechte Security	[4.18]
Desjardins	20. Jun	2.900.000	inside job	[4.19]
2019 Bulgarian revenue agency hack	16. Jul	5.000.000	hacked	[4.20]
Capital One	29. Jul	106.000.000	hacked	[4.21]
StockX	03. Aug	6.800.000	hacked	[4.22]
Health Care Image Leak	17. Sep	16.000.000	ungeschützt	[4.23]
Novaestrat	18. Sep	20.000.000	ungeschützt	[4.24]
Mobile TeleSystems (MTS)	20. Sep	100.000.000	Fehlkonfiguration/schlechte Security	[4.25]
Amazon Japan G.K.	26. Sep	unknown	versehentlich hochgeladen	[4.26]
DoorDash	26. Sep	4.900.000	hacked	[4.27]
Zynga	30. Sep	218.000.000	hacked	[4.28]
Insgesamt:		**4.174.339.740**		

Fazit

Trotz neuer Vorschriften, der Verfügbarkeit modernster Technologie und einem besseren Verständnis von Cyberrisiken, gab es 2019 eine unglaubliche Anzahl von hochgradigen Datenlecks. Weil auf dem kriminellen Markt mehr Informationen als je zuvor verfügbar sind, ist der Datenschutz für die große Mehrheit der Unternehmen ein Thema von höchster Priorität geworden.

Da 80% der Datenschutzverletzungen auf unbeabsichtigtes oder schuldhaftes Verhalten von Mitarbeitern zurückzuführen sind, müssen Unternehmen ihre Datenverarbeitung genau unter die Lupe nehmen, um die Ursache zu ermitteln. Mitarbeiterschulungen, Überwachung und interne Bedrohungsanalysen sind der Schlüssel zur Verhinderung von Datenlecks.

Prominente Fälle wie Marriott, British Airlines und Facebook zeigen deutlich die Konsequenzen für Organisationen. Nicht nur die Reputation kann ernsthaften Schaden nehmen. Auch die Regulierungsbehörden lassen zunehmend ihre Muskeln spielen und verhängen erschreckende Bußgelder. Die Wellen, die von diesen Ereignissen ausgehen, stoppen nicht bei der betroffenen Organisationen, Datenschutzverletzungen sind jetzt für viele Menschen eine neue Realität. Die Betroffenen finden sich plötzlich auf der Jagd nach der Kontrolle ihrer eigenen digitalen Identität wieder.

Der COVID-19-Lockdown hat einen beträchtlichen Teil der Dienstleistungsbranche zur Heimarbeit gezwungen. Infolgedessen hat die Bedeutung der sicheren Datenübertragung, der Speicherung in der Cloud und des Zugriffs von außerhalb des Perimeters einen neuen Höhepunkt erreicht. Auch wenn schnelles Handeln erforderlich war, ist es von entscheidender Bedeutung, dass Unternehmen ihre Sicherheit schnell an die neue Situation anpassen und es vermeiden, Datendieben neue Angriffsflächen zu bieten. Dies kann aber auch als eine Gelegenheit gesehen werden, um den Datenschutz im Allgemeinen zu überdenken.

Organisationen sehen sich bei der Nutzung digitaler Plattformen erheblichen Cyber-Risiken ausgesetzt. Die Besten werden die Gelegenheit nutzen und unter schwierigen Bedingungen widerstandsfähig bleiben. Diejenigen, die nicht früh genug geeignete Schutzmaßnahmen identifizieren, nehmen erhebliche Risiken in Kauf und werden mit zunehmenden Betriebsstörungen rechnen müssen.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Technology Review

Wie sicher ist VPN?

Virtual private networks (VPN) gelten als sicheres Kommunikations- und Datenübertragungsmittel, insbesondere in der Geschäftswelt. Wir haben genauer hingeschaut.

Unternehmen statten ihre Mitarbeiter mit mobilen Geräten wie Laptops und Smartphones aus, damit sie ihre täglichen Aufgaben erledigen können. Dies macht die Belegschaft viel mobiler, stellt aber eine implizite Belastung für die Mitarbeiter dar: die Sicherstellung, dass sie immer online sind. Die Sicherheit wird durch das zugrunde liegende Betriebssystem und unterstützende Lösungen, wie z. B. VPN, gewährleistet. Kommerzielle VPN-Technologie gibt es seit mindestens 1996. Vor kurzem hat diese Technologie eine neue Bedeutung erlangt, da Millionen von Mitarbeitern weltweit aufgrund des COVID-19-Lockdowns per Fernzugriff auf Unternehmensnetzwerke zugreifen mussten.

VPN-Lösungen, insbesondere der Enterprise-Klasse, können durch verschiedene Konfigurationsoptionen kompliziert und nuanciert sein. Die Remote-Unterstützung von Benutzern mit technischen Problemen kann bei dem Versuch, diese durch falsch konfigurierte Lösungen entstehenden Probleme zu lösen, zu Mehraufwand führen.

In diesem Abschnitt werden wir die Ergebnisse unserer Recherchen über die Wirksamkeit moderner kommerzieller VPN-Lösungen, im Hinblick auf aktuelle Anwendungsfälle, typische Endpoint-Technologien und aktuelle Bedrohungsmodelle vorstellen.

Apropos VPNs - funktionieren sie eigentlich noch?

Was soll ein VPN leisten?

Ein VPN sollte seinen Nutzern Vertraulichkeit und Integrität der Netzwerkverbindung bieten und vor Datenspionage und Manipulation schützen. In Unternehmensumgebungen werden Authentifizierung und Zugriffskontrolle hinzugefügt, um sicherzustellen, dass nur berechtigte Benutzer Zugriff auf Unternehmensressourcen erhalten. In diesem Sinne erfüllen moderne Unternehmens-VPNs mindestens zwei, getrennte Anwendungsfälle.

Die Worte virtuell, privat und Netzwerk fassen genau das zusammen, was ihr Zweck ist. "Virtuell" bezieht sich auf die Tatsache, dass das Konstrukt, das es nachahmt, einem physischen Äquivalent ähnelt und sich wie dieses verhält. Das Wort "privat" erhebt Anspruch auf Vertraulichkeit und impliziert Vertrauenswürdigkeit.

Daraus lässt sich ableiten, dass ein VPN eine logische Erweiterung eines privaten Netzwerks zu einem anderen Standort ist und den Eindruck vermittelt, dass sich ein entferntes Computergerät im lokalen Netzwerksegment befindet. Diese Netzwerkerweiterung kann sich über das öffentliche Internet erstrecken.

VPN ist nicht einfach

Die Realität von VPN-Lösungen besteht darin, dass sie selten auf einfache Weise eingesetzt werden, da der gesamte Datenverkehr über das VPN zum Unternehmen geleitet wird. Bei den meisten Implementierungen ist es beispielsweise möglich, einen Teil des Datenverkehrs durch den VPN-Tunnel zu leiten, während das andere Teil des Datenverkehrs direkt an das Internet gesendet wird. Diese Möglichkeit wird oft als "Split-Tunneling" bezeichnet und hat sich mit steigenden Internetgeschwindigkeiten immer mehr durchgesetzt.

Ein weiteres komplexes Beispiel betrifft die Remote-Mitarbeiter, die sich mit kostenlosen Internet-Hotspots verbinden, die normalerweise von Cafés, Flughäfen, Hotels usw. angeboten werden. Hotspots sind Wi-Fi-Zugangspunkte, die freie Internet-Bandbreite bieten. Die meisten Hotspots haben heute ein Captive Portal, das entweder ein Passwort, einen Gutscheincode oder irgendeine Form der Zustimmung verlangt, bevor es einem angeschlossenen Computer den Zugang zum Internet erlaubt.

Eine robuste VPN-Implementierung sollte es einem Benutzer nicht ermöglichen, mit einer Netzwerkressource zu interagieren, die den VPN-Tunnel umgeht. In den meisten modernen Implementierungen führt dies jedoch zu einem Catch 22-Szenario, da der Benutzer zunächst eine Verbindung zum Hotspot herstellt und dann die Anforderungen des Portals verarbeiten muss, bevor die VPN-Software eine Verbindung zum Server herstellen und den Tunnel aufbauen kann.

Was passiert in der Zeitspanne zwischen der Verbindung zum Wi-Fi-Hotspot und der Aktivierung des VPN, während der Benutzer mit dem Captive Portal zu tun hat?

Wie verletzlich ist der Benutzer während dieser Zeit? Der Wi-Fi-Hotspot isoliert Gäste sicher, während die lokale Firewall auf dem Laptop den Benutzer vor jedem Angreifer schützt; aber funktioniert das auch dann, wenn sich der Hotspot vollständig unter der Kontrolle eines Angreifers befindet?

VPNs & Security

Für diese Forschung ist es wichtig, die grundlegenden Bedrohungen gegen Vertraulichkeit, Integrität und Zugangskontrolle zu verstehen, vor denen das VPN den typischen Firmenanwender schützen soll:

DNS ‘Person in the middle’ (PiTM) oder Spoofing

Der Angreifer speist irgendwie gefälschte DNS-Antworten auf legitime Anfragen des Benutzers ein und kontrolliert so, wo die nachfolgende Verbindung letztendlich endet. Dies ist ein Vorläufer für mehrere andere Angriffe, wie gefälschte Websites zum Auslesen von Credentials oder "Responder"-Angriffe (siehe unten).

Anmeldedaten sammeln über gefälschte Website

Sobald der Angreifer DNS und Routing kontrolliert (wie mit einem bösartigen Access Point), kann er dem Benutzer eine gefälschte Anmeldeseite zu wertvollen Ressourcen wie O365 präsentieren, um Anmeldedaten zu sammeln.

Erfassen von Windows-Hashes über Responder

Bei so genannten "Responder"-Angriffen werden Windows-Systeme so ausgetrickst, dass sie sich mit einem gefälschten Windows-Dienst verbinden, der wiederum eine Authentifizierung anfordert und dann den gesendeten Passwort-Hash erfasst. Dies ermöglicht weitere Angriffe auf Active Directory-Ressourcen, wie z.B. die Verbindung zum VPN-Gateway, das üblicherweise Active Directory zur Authentifizierung verwendet.

Verwendung des Browsers als Tunnelling-Proxy

Sobald der Angreifer DNS und Routing kontrolliert (wie mit einem böswilligen AP), kann er JavaScript-Code in andere legitime Websites einschleusen, um eine gewisse Fernsteuerung über den Computer des Opfers auszuüben, z.B. indem er ihn als Drehpunkt verwendet, um den Datenverkehr in das Unternehmensnetzwerk zu tunneln.

Verwendung von IPv6 zur Interaktion mit dem Host

Die meisten Unternehmens-VPN-Technologien sind für den Schutz des IPv4-Verkehrs ausgelegt, aber auf vielen Endpunkten laufen inzwischen auch IPv6-Stacks, die für die Kommunikation im LAN und Internet genutzt werden können. Wenn das VPN IPv6 nicht kontrolliert wird, bietet dies dem Angreifer einen offenen Kanal für die Kommunikation mit dem Computer.

Alle oben beschriebenen Angriffe können als durchführbar betrachtet werden, wenn ein Firmencomputer mit einem öffentlichen Wi-Fi-Zugangspunkt (AP) verbunden ist, der von einem Hacker kontrolliert wird. Angesichts des unklaren Zustands, in welchen Captive Portals die Endpoints bringen, wollen wir wissen, inwieweit VPNs noch die Art von Schutz bieten, die wir voraussetzen.

Captive Portals

Captive Portals werden häufig von Wi-Fi-Zugangsanbietern wie Hotels, Flughäfen und Cafés genutzt. Ein Gerät, das einen Internetzugang benötigt, kann sich mit dem Wi-Fi-Netzwerk verbinden, hat aber in der Regel erst dann Zugang zum Internet, wenn die Forderungen des Portals nach Zahlung, persönlichen Daten oder Zustimmung erfüllt sind.

Sobald das Betriebssystem (OS) der meisten modernen Geräte mit einem Wi-Fi-Access Point verbunden ist, testet es im Allgemeinen den Internetzugang, indem es eine HTTP-Anfrage an eine URL seiner Wahl stellt. Wenn die HTTP-Antwort mit dem übereinstimmt, was es erwartet, geht das Betriebssystem davon aus, dass das Gerät mit dem Internet verbunden ist.

Wenn jedoch ein Captive Portal angetroffen wird, fragt das Betriebssystem den Benutzer ab, in der Regel durch eine Webbrowser-Schnittstelle, die eine Nachricht vom Portal in Form eines Webformulars anzeigt. Im Fall von Android und iOS wird der Benutzer darüber informiert, dass ein Captive Portal vorhanden ist, und gefragt, ob er mit diesem interagieren möchte.

Android und iOS haben spezielle Webbrowser eingebaut, die so genannten Captive Portal Mini-Browser. Diese sind von den vollwertigen Webbrowser-Apps getrennt. MacOS hat ein ähnliches Konzept in Form eines Captive Network Assistant.

Windows und Linux sind jedoch auf den Standard-Webbrowser angewiesen, um mit dem Captive Portal zu interagieren. Windows kann den Standard-Webbrowser automatisch starten, wenn es ein Captive Portal erkennt.

Linux ist darauf angewiesen, dass der Benutzer selbstständig einen Webbrowser startet, der ein Captive Portal erkennen kann.

VPN Split-Tunnelling

Eine andere übliche, wenn auch nicht notwendige VPN-Konfigurationseinstellung, die von Unternehmen verwendet wird, heißt 'Split-Tunneling'. Beim Split-Tunneling wird das VPN so konfiguriert, dass nach der Verbindung bestimmte Netzwerkanforderungen durch den VPN-Tunnel geleitet werden, während der übrige Datenverkehr den Standardregeln für das Netzwerk-Routing folgt. Dies geschieht, damit nur der für das Unternehmensnetzwerk bestimmte Datenverkehr verschlüsselt wird und einer Zugangskontrolle unterliegt, während das reguläre lokale Netzwerk- oder Internet-gebundene Verkehr direkt und ungestört übertragen werden kann.

Der Grund dafür liegt auf der Hand - um den Zugang zu Ressourcen in lokalen Netzwerken zu ermöglichen und die Leistung beim Zugriff auf öffentliche Internetseiten und -dienste zu verbessern. Die Auswirkungen dieser Konfigurationswahl sind jedoch möglicherweise nicht so klar, da sie auch impliziert, dass ein Computer, der von einem böswilligen Wi-Fi-Netzwerk "gefangen" wurde, gezwungen werden könnte, Verbindungen herzustellen oder Datenverkehr über unverschlüsselte und ungeschützte Verbindungen zu senden.

Bei unseren Tests von zwei großen VPN-Produkten für Unternehmen, umfasste die Standardeinrichtung nach der Einrichtung des VPN auch Split Tunneling. Dies ist das Modell, das wir in unseren Tests verwendet haben und über das wir unten berichten.

Test A: Standardmodus

Wie vermutet, ist der typische Windows-Computer in diesem Zustand für beide von uns getesteten VPN-Produkte anfällig für alle von uns beschriebenen Angriffe. Noch beunruhigender ist, dass beide VPN-Produkte bei Verwendung von Split-Tunneling auch dann noch anfällig für diese Angriffe sind, wenn das VPN vollständig eingerichtet ist. (✓ = geschützt, ✗ = kein Schutz)

Angriffsmuster	Captured		Online	
	VPN1	VPN2	VPN1	VPN2
DNS ‘Person in the middle’ oder Spoofing	✗	✗	✗	✗
Anmeldedaten sammeln über gefälschte Website	✗	✗	✓	✓
Erfassen von Windows-Hashes über Responder	✗	✗	✗	✗
Verwendung des Browsers als Tunneling-Proxy	✗	✗	✓	✓
Verwendung von IPv6 zur Interaktion mit dem Host	✗	✗	✗	✗

Die obigen Ergebnisse stellen die Ergebnisse einer vereinfachten und eigenständigen Version jeden Falles dar. Sowohl für die fehlgeschlagenen als auch für die erfolgreichen Tests kann es Fälle geben, in denen die Ergebnisse aufgrund anderer Umstände, die über den Rahmen dieses Tests hinausgehen, abweichen können.

Lockdown-Modus

Moderne VPN-Technologien haben auf die oben beschriebene Herausforderung der Captive Portals reagiert, indem sie eine Reihe von Funktionen eingeführt haben, die allgemein als "Captive Portal Remediation" oder "Lockdown-Modus" bekannt sind und in bestimmten nicht vertrauenswürdigen Umgebungen einen besseren Schutz bieten sollen.

Der Lockdown-Modus kann als eine Reihe von VPN-Funktionen betrachtet werden, die dazu dienen, die Menge des Datenverkehrs zu begrenzen, die den Endpoint verlässt, während er sich im WLAN befindet und sich mit dem Captive Portal befasst.

Die Besonderheiten dieser Merkmale sind von Produkt zu Produkt unterschiedlich, aber im Allgemeinen belaufen sie sich auf

- den Schutz des Browsers, der sich mit dem Portal verbindet
- Begrenzung der Menge des Datenverkehrs, die den Computer verlassen darf.

Wir haben daher die beiden VPN-Produkte, die diese Funktionen bei vollem Funktionsumfang bieten, getestet, um festzustellen, wie wirksam ihr Schutz ist.

Test B: Lockdown-Modus

Zusammenfassend zeigen unsere Tests, dass selbst die so genannten "Lockdown"-Funktionen, die von den VPN-Anbietern zur Minderung der von Captive Portals verursachten Risiken bereitgestellt werden, wenig zur Minderung der heutigen technischen Bedrohungen beitragen. (✓ = geschützt, ✗ = kein Schutz)

Angriffsmuster	Captured		Online	
	VPN1	VPN2	VPN1	VPN2
DNS 'Person in the middle' oder Spoofing	✗	✗	✗	✗
Anmeldedaten sammeln über gefälschte Website	✗	✗	✓	✓
Erfassen von Windows-Hashes über Responder	✗	✓	✗	✗
Verwendung des Browsers als Tunneling-Proxy	✓	✗	✓	✓
Verwendung von IPv6 zur Interaktion mit dem Host	✗	✗	✗	✗

Die obigen Ergebnisse stellen die Ergebnisse einer vereinfachten und eigenständigen Version jeden Falles dar. Sowohl für die fehlgeschlagenen als auch für die erfolgreichen Tests kann es Fälle geben, in denen die Ergebnisse aufgrund anderer Umstände, die über den Rahmen dieses Tests hinausgehen, abweichen können.

Zusammenfassung der Ergebnisse

Zusammenfassend zeigen unsere Experimente, dass unsere anfänglichen Bedenken hinsichtlich des Versagens von VPNs zum Schutz in Captive Portals alle zutreffen. Das heißt nicht, dass diese VPNs nicht "funktionieren" oder dass sie "Bugs" haben, sondern vielmehr, dass Captive Portals einen Anwendungsfall darstellen, für den VPNs ursprünglich einfach nicht vorgesehen waren.

Unter der Annahme, dass jeder "kostenlose" Wi-Fi-Dienst vernünftigerweise als bösartig betrachtet werden sollte, und unter Berücksichtigung der heutigen Angriffsvektoren und Tools erweist sich diese Unfähigkeit, mit einem bedeutenden neuen Anwendungsfall umzugehen, als ernsthafte Einschränkung. Sie zwingt uns, uns bei der Verteidigung des mobilen Endpoints auf sekundäre Mechanismen wie SSL/TLS, Firewalls und Endpoint Protection zu verlassen.

Enttäuscht mussten wir außerdem feststellen, dass ein unvorsichtig konfiguriertes VPN, selbst wenn es vollständig eingerichtet ist, kaum besser mit diesen sehr realen Bedrohungen umgehen kann.

Als Antwort auf die Herausforderungen, die durch Captive Portals eingeführt wurden, haben Unternehmens-VPNs eine Reihe von Lockdown-Funktionen eingeführt, die die Probleme "mildern" sollen. Diese Funktionen gehen in der Tat einige Probleme an, aber leider zeigen sie kaum Wirkung auf die Gesamtheit der Bedrohungen, die wir für unsere Experimente in Betracht gezogen haben.

Auch wenn uns das Verhalten einiger dieser Funktionen bisweilen verwirrt hat, müssen wir betonen, dass es sich hierbei wieder einmal um eine grundlegende Eigenschaft, der Funktionsweise von Captive Portals und nicht um ein Problem mit den Produkten selbst handelt.

Die Bedrohungen, die wir in unseren Experimenten betrachtet haben, sind keineswegs katastrophaler Natur. Mehrere Faktoren müssen zusammenkommen, damit die Schwächen ausgenutzt werden können, und mehrere externe Faktoren könnten den Erfolg solcher Angriffe verhindern.

Wir behaupten jedoch, dass es eine realistische Reihe von Bedingungen gibt, unter denen moderne VPNs ihr erklärtes Ziel der Sicherung von Vertraulichkeit, Integrität und zuverlässiger Zugangskontrolle grundsätzlich nicht erfüllen können.

Wie unsere eigenen Erfahrungen aus erster Hand zeigen, können die Bedingungen, die erforderlich sind, um diese Schwäche der VPN-Technologien böswillig auszunutzen, unter gewöhnlichen realen Umständen auftreten und sind wahrscheinlich viel häufiger, als uns bewusst ist.

Wir würden behaupten, dass die Bedrohung ernst und realistisch genug ist, um eine Reaktion der IT-Teams von Unternehmen zu rechtfertigen, wie wir weiter unten erörtern werden.

Empfehlungen

Wir glauben, dass die in diesen Experimenten beschriebenen Schwachstellen und Bedrohungen ernst genug sind, um eine dringende Reaktion zu rechtfertigen, aber diese muss nicht unbedingt teuer oder störend sein.

Unsere technischen Empfehlungen lassen sich wie folgt zusammenfassen:

Konfigurationsänderungen:

- Vermeiden Sie die Verwendung von Split-Tunneling in Ihrer VPN-Konfiguration. Lassen Sie stattdessen ihre Mitarbeiter durch das Unternehmensnetzwerk tunneln, wo der Datenverkehr der Ausgangsfilterung, Monitoring und anderen Schutzmaßnahmen unterzogen wird, die das interne Netzwerk bietet.
- Verwenden Sie Ihre VPN-Konfiguration, um die Nutzung eines internen DNS-Servers, den sie selbst kontrollieren, zu erzwingen und das DNS-Domänensuch-Suffix fest zu codieren. Beide von uns getesteten VPN-Produkte bieten das an, und wir gehen davon aus, dass auch andere seriöse Produkte diese Funktion bieten.
- Verstehen und implementieren Sie alle Funktionen, die Ihre VPN bietet, wie 'Lockdown' und 'Captive Portal Mitigation'. Dies ist allerdings keine so einfache Änderung und erfordert sorgfältiges Testen und Deployment.

Andere technische Kontrollen:

- Stellen Sie sicher, dass alle internen Windows-Systeme, auf die Ihre Benutzer zugreifen, voll qualifizierte Hostnamen verwenden. Verwenden Sie zum Beispiel konsequent 'ocd-src-server.ocd.local' und nicht nur 'ocd-src-server'.
- Lokale Host-Firewalls und hochentwickelte Endpoint Detection & Protection-Programme können bei richtiger Anwendung einen erheblichen Schutz gegen die hier beschriebenen Angriffe bieten.

Strategische Ansätze:

"If you're not the customer you're the product" ist ein Sprichwort, das heutzutage häufig verwendet wird.

Wir glauben, dass dies auch für sogenannte "free" Wi-Fi-Dienste gilt. Die Kosten für Privatsphäre und Sicherheit, die im Austausch gegen kostenloses Internet für mobile Nutzer angeboten werden müssen, sind unserer Meinung nach zu hoch für moderne Unternehmen, die beide wesentlichen Aspekte ernst nehmen müssen. Wir empfehlen daher, dass Unternehmen mobile Mitarbeiter mit geeigneten mobilen Datentechnologien und Bandbreiten ausstatten, so dass sie sich über einen relativ vertrauenswürdigen, sichtbaren und rechenschaftspflichtigen Mobilfunknetzbetreiber verbinden können, und nicht über ein wahres Sammelsurium völlig unbekannter kostenloser Internetanbieter, deren Integrität und Motiv niemals vollständig vertraut werden kann.

Erwägen Sie Zero Trust.

Zero Trust ist ein sich entwickelndes Sicherheitsparadigma, bei dem alle Netzwerke als gleichwertig und nicht vertrauenswürdig betrachtet werden, bei dem es keinen internen oder externen Raum gibt und bei dem daher Sicherheit auf dem Endpoint und auf dem Server erreicht werden muss, ohne dass ein VPN erforderlich ist. Zero Trust ist eine Sicherheitsideologie, die für das moderne Internet konzipiert wurde und von Vorreitern wie Google in deren eigene Sicherheitsstrategie übernommen wird. Wir empfehlen unseren Kunden, sich ernsthaft mit dem Zero-Trust-Konzept und den neuen Technologien und Ansätzen auseinanderzusetzen, wenn die Security relevant bleiben soll, angesichts der sich ändernden Technologien und aufkommenden Bedrohungen in den nächsten fünf bis zehn Jahren.

Fazit

Sicherheitstechnologien kommen üblicherweise als Antwort auf eine bestimmte Art von Bedrohungen auf den Markt.

In dem Maße, wie sich die Bedürfnisse des Kunden und die Technologielandschaft entwickeln, muss sich auch ein Sicherheitsprodukt weiterentwickeln. Die Gewährleistung einer kontinuierlichen Abstimmung zwischen den sich entwickelnden Bedrohungen und den Technologien, die wir zu ihrer Eindämmung einsetzen, erfordert ständige Wachsamkeit.

Der COVID-19-Lockdown hat einmal mehr bewiesen, wie sehr wir auf sichere Netzwerktechnologie angewiesen sind. Dadurch ist VPN in den Fokus sowohl von potenziellen Angreifern als auch von verantwortlichen Sicherheitsbeauftragten gerückt.

Unsere Untersuchung über die Wirksamkeit von VPN-Produkten im Kontext moderner Internet-Konfigurationen gibt Anlass zur Besorgnis. Dazu kommt noch, dass es gewisse Bemühungen erfordert, die Bedrohung zu durchschauen, dass es schwierig ist, zu verstehen, wie unsere Security Tools auf die Bedrohung abgestimmt sind, und dass wir letztlich sicherstellen müssen, dass wir diese Tools in vollem Umfang nutzen. Keine Technologie allein lässt ein Problem verschwinden.

Das liegt in unserer Verantwortung und ist unser Job, der dadurch natürlich nicht gerade einfacher wird.

Double-Dip: Geldstrafen für Firmen nach Datenleck

British Airways wurde im Rahmen der GDPR mit einer Geldbuße in Höhe von 183 Millionen Pfund aufgrund des Verstoßes im Jahr 2018 belegt [t32], Equifax muss ganze 700 Millionen US-Dollar als Ausgleich für die Datenpanne im Jahr 2017 zahlen [t33] und Marriott muss nach dem Datenklau bei Starwood mit einer Geldstrafe in Höhe von 123 Millionen US-Dollar rechnen [t34].

JUL

Ransomware eCh0raix/QNAPCrypt zielt auf Netzwerkspeicher

In Linux-basierten Netzwerken zielt die Malware auf NAS-Server, die von QNAP Systems produziert werden, entweder durch das Erzwingen schwacher SSH-Zugangsdaten oder durch das Ausnutzen bekannter Schwachstellen [t35].

Der Staat Kasachstan könnte PiTM-Angriffe auf alle Bürger starten

Kasachische ISPs sind gezwungen, ein von der Regierung ausgestelltes Stammzertifikat mit der Bezeichnung "National Security Certificate" bei ihren Kunden installieren zu lassen, wodurch die Behörden in die Lage sind, alle verschlüsselten HTTPS- und TLS-Verbindungen abzufangen und zu zensieren [t36].

Ransomware verursacht Stromausfälle in Johannesburg

Die größte Stadt Südafrikas mit mehr als 5 Millionen Einwohnern litt mehrere Tage lang unter Stromausfällen, da ihr wichtigster Stromversorger, City Power, von einem Ransomware-Angriff getroffen wurde [t37].

AUG

Europäische Zentralbank schließt 'BIRD-Portal' nach Hacking-Angriff

"Unbefugten" war es gelungen, die Website des Banks' Integrated Reporting Dictionary (BIRD), die von einem Drittanbieter gehostet wurde, zu hacken, was die EZB schließlich zwang, die Website stillzulegen [t39].

POC: Ransomware kann sich auf DSLR-Kameras ausbreiten

Forscher von Check Point haben große Schwachstellen in der Firmware von Canon-Kameras entdeckt. Ein POC hat gezeigt, dass diese leicht ausgenutzt werden könnten, um eine Kamera über USB oder Wi-Fi mit Ransomware zu infizieren [t38].

Französische Polizei entfernte RETADUP-Malware per Fernzugriff von 850.000 infizierten PCs

Die französische Gendarmerie Nationale hat ein RETADUP-Botnet mit Hilfe eines Fehlers in der CNC-Kommunikation der Malware außer Gefecht gesetzt. Die Abteilung für Cyberkriminalität (C3N) stellte die Kontrolle über den CNC-Server ein und löste eine Selbstzerstörung der Malware auf infizierten Clients aus [t40].

Ransomware befällt Dienstanbieter für Ransomware-Schutz

DDS Safe, ein cloud-basiertes Datensicherungssystem, das in Zahnarztpraxen in den USA sehr beliebt ist (um medizinische Aufzeichnungen vor Cyberattacken zu schützen), wurde von der Ransomware Sodinokibi getroffen [t41].

Michael Haugland
Threat Research Analyst
Orange Cyberdefense

Technology Review

Die PKI und Digital Trust

Die Public Key Infrastructure (PKI), die wir heute verwenden, erleichtert viele unserer sicheren, alltäglichen Internetaktivitäten: E-Commerce, Internetbanking, Instant Messaging und vertrauliche E-Mails. PKI kann auf verschiedene Weise genutzt werden, um die vier Zutaten für Vertrauen zu schaffen, nämlich: Vertraulichkeit, Authentifizierung, Integrität und Nachweisbarkeit. Es ist etwas, das wir für selbstverständlich halten und das wir fast nie in Frage stellen.

In seliger Unwissenheit akzeptieren wir, dass es einfach funktioniert. Aber tut es das auch wirklich?

Wir haben die grundlegenden Bausteine der PKI analysiert, um zu verstehen, wem wir tatsächlich vertrauen, wenn wir verschlüsselte Datenübertragungen wie das sichere Hypertext Transfer Protocol, kurz HTTPS, verwenden.

Was wir festgestellt haben, ist alarmierend: Digital Trust ist nicht nur geografisch sehr ungleich verteilt (es ist in den USA weitgehend hoch), sondern Sie vertrauen auch Ländern, die Ihnen wahrscheinlich Sorgen bereiten würden.

Offenbar ist die Grundlage einer sicheren Online-Kommunikation unser Vertrauen in weitgehend unüberwachte, intransparente private Organisationen. Und niemand denkt jemals darüber nach.

Wir vertrauen auf Zertifikate

Die Verwendung der Verschlüsselung geht auf die Zeit vor den Römern zurück und wurde sogar von Caesar popularisiert. Das Grundkonzept ist einfach und hat sich seit Jahrtausenden nicht geändert: Die Verwendung eines geheimen Schlüssels, um eine Nachricht in einen Chiffriertext umzuwandeln, macht es für jeden, der nicht im Besitz des geheimen Schlüssels ist, unmöglich, ihn zu entziffern.

Mit der PKI können wir dies für HTTPS-Verkehr leicht erreichen:

- Wir verbinden uns mit einem Webserver, der sich mit einem digitalen Zertifikat identifiziert;
- Unser Browser überprüft, ob das digitale Zertifikat gültig ist (Domain, Datum und von einer Certificate Authority (CA) signiert);
- Wenn es validiert ist, werden kryptographische Schlüssel ausgetauscht, und die resultierende Kommunikation wird verschlüsselt.

Die Möglichkeit, dass sich die Parteien gegenseitig mit digitalen Zertifikaten identifizieren können, ist die Grundlage für eine zuverlässige Kommunikation, die Vertraulichkeit durch Verschlüsselung, Datenintegrität und eine vernünftige Grundlage für die Nachweisbarkeit bietet.

Wenn wir digitalen Zertifikaten vertrauen, verlassen wir uns auf unabhängige CAs, die sie verteilen. Wir vertrauen darauf, dass sie bestimmte Prinzipien und Kriterien erfüllen, um eine Certificate Authority zu werden. Wir (Endnutzer) spielen bei der Auswahl der CAs keine Rolle und verlassen uns darauf, dass der Abonnent (Eigentümer) des digitalen Zertifikats eine geeignete CA auswählt, wenn wir ihr Produkt oder ihren Dienst für unsere Kommunikation verwenden. Die von uns verwendeten Geräte und die von uns gewählte Software ist mit CAs vorinstalliert, die in unserem Namen Vertrauen schaffen, indem das Vorhängeschloss angezeigt wird, um auf vertrauenswürdige und sichere Kommunikation hinzuweisen.

Also, wem vertrauen Sie? Und was bedeutet das für eine sichere Geschäftskommunikation?

Erzwungenes Vertrauen

Eine PKI besteht aus allen Rollen, Richtlinien und Verfahren, die zum Verwalten (Erstellen, Verteilen, Speichern und Widerrufen) digitaler Zertifikate notwendig sind. Die Implementierung dieser Zertifikate wird in der Regel von einem Territorium oder einer Region geregelt, was oft ihre eigentlichen Prinzipien bricht.

Vertrauen erfordert jedoch Zuverlässigkeit, Konsistenz und Transparenz: Das direkte Gegenteil der sich entwickelnden PKI-Implementierung. Dieser Konflikt ist eher ein konzeptionelles Dilemma als ein technischer Fehler in der PKI, was die Behebung noch schwieriger macht.

Die CAs sind die Ursache dieses Problems. Zertifikate sind die Ausweise des Internets. Aber stellen Sie sich vor, was passieren würde, wenn Personalausweise nicht ausschließlich von vertrauenswürdigen Regierungsorganisationen ausgestellt werden würden, sondern stattdessen von einer undurchsichtigen Gruppe privater Institutionen, jede nach ihren eigenen Regeln und ihrer eigenen Agenda.

Einige von ihnen würden offiziell vielleicht nicht einmal mehr existieren, aber ihre Ausweise würden immer noch verwendet werden. Welche Auswirkungen hätte dies auf die Vertrauenswürdigkeit von Personalausweisen? Wäre es klug, einem Boten mit geschäftskritischen Informationen zu betrauen, der sich auf einen solchen Ausweis beruft?

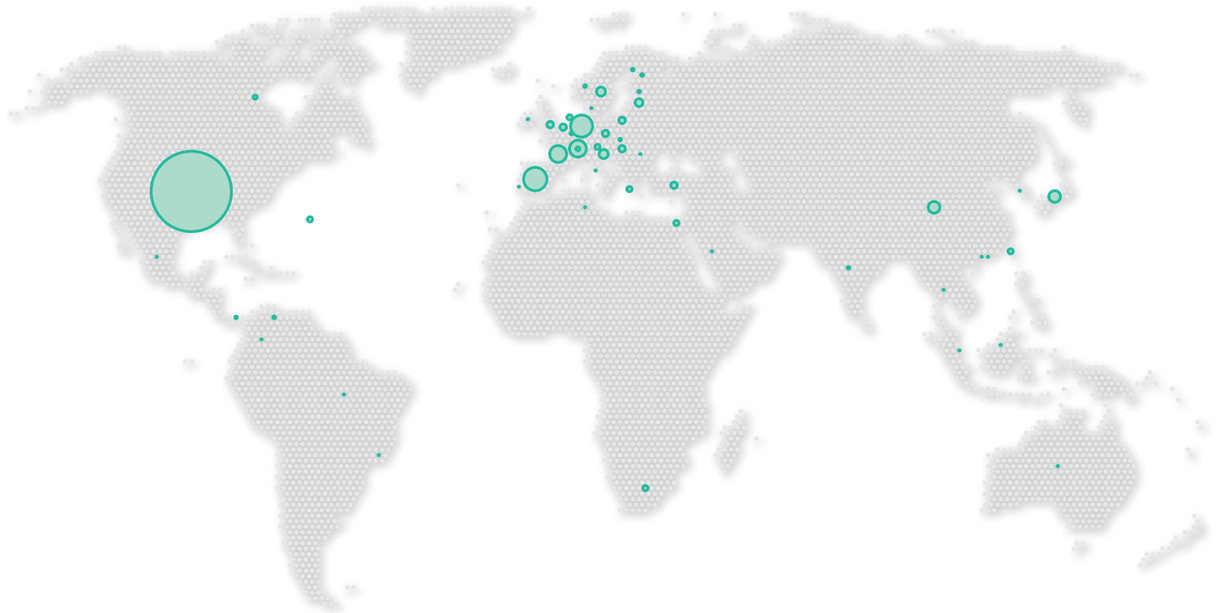
Doch so funktioniert die PKI heute im Großen und Ganzen.

Wem vertrauen wir da eigentlich?

Unsere Methodik

Wir nutzten "The Alexa Top Sites Service", einen Dienst, der Zugang zu Listen von Websites bietet, die nach dem Alexa Traffic Ranking von Amazon geordnet sind. Diese Liste bietet einen guten Durchschnitt des Ökosystems des Webs als Ganzes.

Wir haben uns mit Hilfe eines proprietären Tools mit jeder Website auf der "Liste" (~1 Million) verbunden und die gesamte Zertifikatskette heruntergeladen.

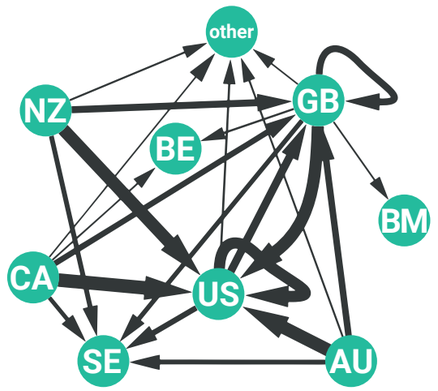


Geografische Verteilung der Trust Store-Zertifikate

Die obige Karte wurde erstellt, indem der Trust-Store nach allen Quellen durchsucht und die Zertifikate nach dem im Zertifikat selbst definierten Ländercode (Attribut C) gruppiert wurden. Jedes Land wurde auf eine Koordinate abgebildet und auf der Karte mit einer Kreisgröße eingezeichnet, die proportional zur Anzahl der Zertifikate in jeder Gruppe ist.

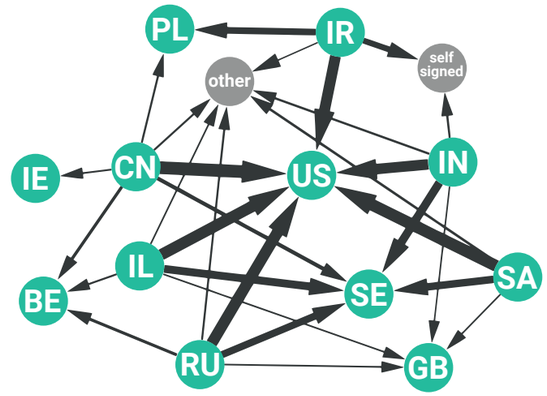
Wem vertrauen die "Five Eyes"?

The Five Eyes, sind ein englischsprachiger Geheimdienstverbund, dem Australien, Kanada, Neuseeland, United Kingdom und die USA angehören. Das Vertrauen unter den FVEY ist sehr stark nach innen gerichtet, oder besser gesagt, auf eine Entität ausgerichtet. Amerika ist mit überwältigender Mehrheit die vertrauenswürdigste Entität. Andere wichtige Standorte sind Großbritannien und Schweden, was nicht sehr überraschend ist. Das scheint seltsam, aber die Root-CAs, die diesen Knoten im Diagramm erzeugt haben, waren ursprünglich Eigentum von AddTrust, sodass die Zuordnung inzwischen eigentlich in die USA weisen sollte (siehe Exkurs: "Wer ist AddTrust").



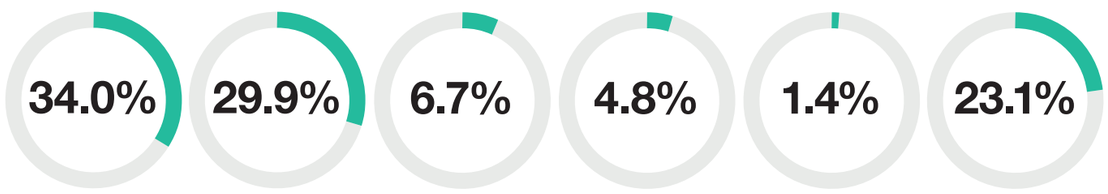
Wem vertrauen die "üblichen Verdächtigen"?

Diese Vertrauensverteilung zeigt zwar ein ähnliches Muster wie die der Five Eyes, in welcher die USA im Epizentrum steht, aber sie zeigt auch einige Abweichungen. Beispielsweise sind selbstsignierte Zertifikate in Indien und Iran übermäßig verbreitet. Darüber hinaus scheinen diese Länder eher dazu geneigt zu sein, Großbritannien, Polen und Belgien ihr Vertrauen zu schenken als die Five Eyes.



Root-CAs nach Nutzung

Meist benutzte Root-Zertifikate innerhalb der analysierten Liste



AddTrust External	DST Root CA X3	Go Daddy Secure Certificate Authority - G2	DigiCert Global Root CA	Self signed	Others (<5%)
AddTrust AB	Digital Signature Trust CO	Go Daddy Group Inc.	Digi Cert Inc.		

Trust Store-Nutzung

Welche automatisch vertrauenswürdigen CAs sind also tatsächlich im Einsatz? Wir analysierten den prozentualen Anteil jedes in der Liste verwendeten Trust Stores. In der untenstehenden Grafik zeigt grün an, welcher Trust Store in der Liste aufgeführt wurde. Um die Auslastung des Trust Stores zu ermitteln, haben wir zwei Werte verglichen:

- Eine Liste der als vertrauenswürdig eingestuften CAs und Root-CAs, die in dem von den Anbietern implementierten Trust Store verfügbar sind
- Die CAs und Root-CAs, die wir nach der Analyse der Liste als "verwendet" identifizieren konnten

"Verwaiste" CAs im System

Wir haben festgestellt, dass große Mengen der vertrauenswürdigen CAs tatsächlich ungenutzt sind. Jede zusätzliche CA stellt eine potenzielle Risikoquelle dar, so dass dies etwas beunruhigend ist. Microsoft zum Beispiel hat etwa 72% seines Trust Stores nicht genutzt.

Mit nur 37% ungenutzten CAs ist Android der effektivste Anbieter. Dies ist allerdings immer noch ein signifikant hoher Prozentsatz.

Wer steckt hinter den CAs?

Wie bereits erwähnt, befinden sich die Stammzertifikate, die CAs identifizieren, in Privatbesitz. Es gibt keine Regulierungsinstanz, die entscheidet, welchen CAs man tatsächlich vertrauen kann.

Während die Zertifikate selbst einem definierten Standard (X.509 [6.1]) unterliegen, ist das Mittel, mit dem eine öffentliche CA ihre Benutzer authentifiziert, nicht vorgesehen. Diese Mittel können erheblich variieren[6.2]. Zwei übliche Arten der Überprüfung sind die grundlegende Domainvalidierung, bei der nur der Domänenbesitz überprüft wird.

Eine erweiterte Validierung würde für mehr Vertrauenswürdigkeit sorgen und tiefer in das eigentliche Unternehmen eindringen, die eine Website oder einen Dienst über HTTPS anbietet, aber sie wird nur selten genutzt. Die einzige Instanz, die tatsächlich eine Art Kontrolle über diese Praktiken und die Vertrauenswürdigkeit von CAs ermöglicht, sind die vier großen Browser: Google/ Chrome, Mozilla/Firefox, Apple/Safari und Microsoft/Edge.

Zu dem Mangel an Transparenz kommt die Tatsache hinzu, dass die CAs ihre Befugnis zur Ausstellung von Zertifikaten an untergeordnete CAs übertragen können (und dies auch tun; diese können sie wiederum an Tochtergesellschaften weitergeben). Dies führt zu einer Zertifikatskette, die bis zur Wurzel zurückverfolgt werden kann. Das macht es jedoch nicht gerade einfacher, herauszufinden, ob die ausgestellten Zertifikate tatsächlich in einem Umfang verifiziert wurden, der das Vertrauen rechtfertigt, das wir in sie setzen. Da es sich um private Organisationen handelt, wäre es auch interessant zu wissen, wem sie tatsächlich gehören.

Um das Ausmaß der Verschleierung zu veranschaulichen, mit der wir in dieser Hinsicht konfrontiert sind, versuchten wir zu untersuchen, welches Unternehmen tatsächlich hinter AddTrust steht, nämlich die Root-CA hinter jedem dritten Zertifikat, auf das wir in der Liste stießen (siehe Exkurs).

Fazit

Etwas stimmt ganz und gar nicht mit der Infrastruktur, der wir unsere Datenverbindungen anvertrauen.

Man kann nur schwer beurteilen, wem man tatsächlich vertraut, selbst wenn man sich ernsthaft damit auseinander setzt.

Sie vertrauen implizit CAs aus Gegenden der Welt, die Sie vermutlich nicht ohne weiteres als vertrauenswürdig einschätzen würden, wenn Sie je gefragt würden.

CAs selbst sind Organisationen, denen es prinzipiell selbst überlassen ist, ob sie verlässlich überprüfen oder nicht, wem sie Zertifikate ausstellen. Aber es gibt keine gemeinsame Kontrollinstanz neben den großen Browsern; und die nutzen einfach die Macht ihrer Marktdominanz, um die Unterstützung für zweifelhafte CAs einzustellen. Ob dies angesichts der entscheidenden Rolle, die Zertifikate bei der sicheren Kommunikation spielen, ausreichend ist, scheint zweifelhaft.

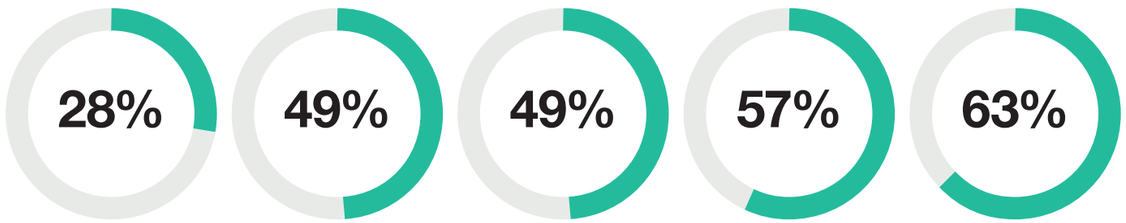
Der Kern des Problems besteht auch darin, dass es für die Endnutzer höchst intransparent ist, wem sie da überhaupt vertrauen.

Wenn wir zum Beispiel AddTrust, einer der häufigsten CAs, vertrauen, vertrauen wir einer Organisation, die eigentlich gar nicht mehr existiert. Deren Stammzertifikate wurden von Comodo, inzwischen als Sectigo bekannt, gekauft. Dies illustriert perfekt den Mangel an Transparenz der PKI.

Und das ist höchstwahrscheinlich nur die Spitze des Eisbergs.

Trust Store Nutzung

Prozentsatz der automatisch vertrauten Root-CAs, die tatsächlich in der Liste benutzt werden



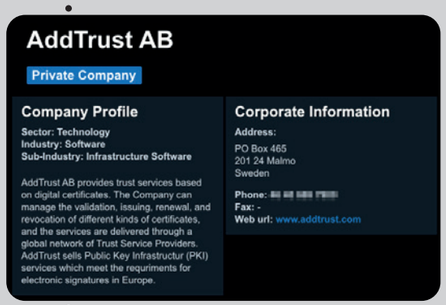
Google, Mozilla, Apple blockieren Kasachstans Root-CA-Zertifikat

Alle größeren Browser warnen nun ihre Benutzer, wenn eine Website versucht, sich mit zweifelhaften, von der kasachischen Regierung ausgestellten Zertifikaten zu authentifizieren [t42].

Exkurs: Wer ist AddTrust?

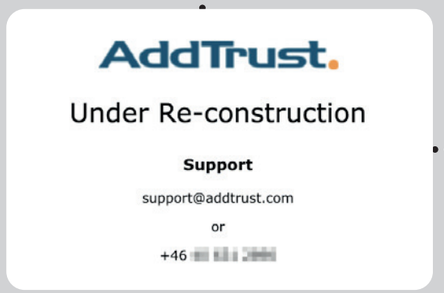
Die Firma "AddTrust" repräsentierte mehr als 30% aller CA-signierten Zertifikate, die aus der Liste gesammelt wurden. Es gibt jedoch nur wenige direkt verfügbare Informationen, die die Glaubwürdigkeit der in Schweden ansässigen Internetfirma untermauern. Das hilft dem ohnehin schon instabilen Ruf der CAs nicht weiter. Hier haben wir versucht, herauszufinden, wer oder was hinter AddTrust steckt.

Wir begannen mit dem Versuch, die Vertrauenswürdigkeit des angeblich in Malmö ansässigen Unternehmens festzustellen, beginnend mit **Bloomberg**[6.2]:

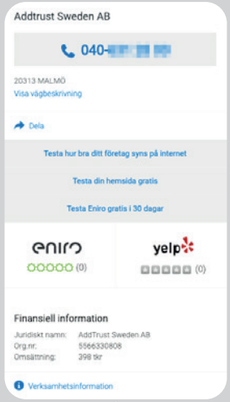


Wir fanden einen Link zur Website des Unternehmens, **www.addtrust.com**, aber diese Seite ist nicht erreichbar.

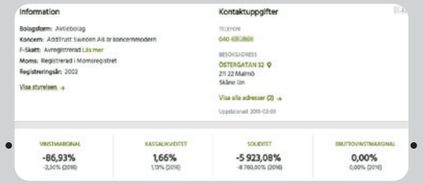
Der letzte Eintrag, den wir für die Website in den Internetarchiven finden können, ist vom 28. Januar 2011[6.3]. Hier sehen wir eine Telefonnummer und eine E-Mail-Adresse **support@addtrust.com**



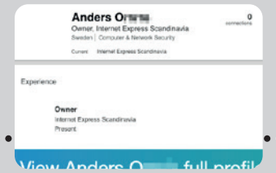
Durch Eingabe der Handelsregister-nummer auf **www.allabolag.se** (die öffentliche Informationen über alle Unternehmen in Schweden auflistet) können wir sehen, dass AddTrust registriert ist unter **"Anders O."**. Die Telefonnummer entspricht der von **Eniro**, und sie gibt uns eine weitere Adresse.



Sucht man auf der schwedischen Website **Eniro** nach dem Unternehmen, erhält man weitere Informationen. Zusätzlich zu einer Telefonnummer haben wir jetzt auch eine schwedische Handelsregisternummer.



Die Überprüfung dieser Adresse in Google Maps führt uns zu einer Firma namens **Lequa AB**.

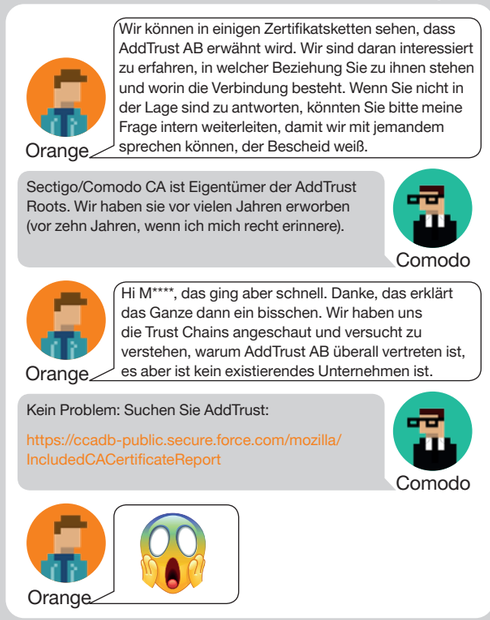


Wir konnten **"Anders O."** auf LinkedIn finden, wo er angibt, der Eigentümer von **"Internet Express Scandinavia (IES)"** zu sein.

Im Abschnitt "Über uns" auf der IES-Website heißt es, dass der Zweck der IES darin besteht, mit ihrem 45%igen Anteil an **Lequa AB** zu arbeiten. Die Domain für Lequa ist **www.lequa.com/**.

Das Produkt, das sie beschreiben, verweist auf diese URL: **http://www.lequinox.com/**, aber diese Domain ist zum Zeitpunkt der Recherche nicht verfügbar

Die IES verwies uns an **Lequa**, die uns ihrerseits an eine Organisation namens **Comodo** verwies, von der wir bereits wissen, dass sie ein wichtiger Akteur in der CA-Landschaft ist[6.4].



Zusammenfassung:

Nach einer intensiven Untersuchung mit obskuren Hinweisen, die über das ganze Netz verstreut sind, haben wir festgestellt, dass AddTrust vor etwa zehn Jahren von Comodo CA gekauft wurde, einer Firma die heute als Sectigo bekannt ist.

Sie stellten ihr letztes Zertifikat im Jahr 2013 aus [6.4]. Aufgrund der langlebigen Trust Chains können wir immer noch sehen, dass AddTrust die Wurzel zahlreicher Zertifikate im Internet ist.

Es ist erwähnenswert, dass die AddTrust External CA Root am

30. Mai 2020 ausläuft [6.5].

Stefan Lager
SVP Global Service Lines
Orange Cyberdefense

Security Prognosen

Anschnallen in Richtung Cyberdefense

Im September 2019 ließ die NASA ein Google-Papier über Quantenüberlegenheit "durchsickern". Es gibt zwar einige Spekulationen darüber, wie (oder warum) dies genau geschehen konnte[7.1], aber eines ist sicher: Quantencomputing nimmt an Geschwindigkeit zu - und es könnte mehr tun, als nur Konzepte wie die Kryptographie beeinflussen. Es könnte in der Tat die Art und Weise, wie Computer funktionieren und wie sie genutzt werden, in einem solchen Ausmaß verändern, dass es die KI-Revolution wie eine kleine Aktualisierung des Betriebssystems aussehen lässt. Wie bei allem im Quantencomputing ist dabei noch nichts wirklich sicher.

Schauen wir uns also verlässlichere Vorhersagen an. Was können wir aus unseren Daten heraus darüber sagen, was 2020 noch auf uns zukommt?

Ein neues Risikomodell

Lange Zeit wurde die Cybersecurity durch einen reaktiven Ansatz vorangetrieben, der sich auf Investitionen in Technologien zur Verhinderung von Cyber-Attacken konzentriert.

Leider hat sich dieser Ansatz als erfolglos erwiesen, da die Zahl der Verstöße trotz höherer Ausgaben für Security zugenommen hat. Wir sind der Meinung, dass es wichtig ist, die Ausgaben auszubalancieren zwischen der Antizipation von Bedrohungen, der Aufdeckung von Sicherheitsverstößen, dem Schutz von Assets, der Reaktion auf Vorfälle und der Wiederherstellung nach Angriffen.

Wir glauben, dass die Unternehmen in Zukunft das Konzept des Cyber-Angriffs in zwei Phasen aufteilen müssen:

1. Der Infrastruktur Breach: Sicherheitslücke bei Geräten oder Workloads;
2. Das Datenleck: Wenn kritische Daten vernichtet werden, für sie Lösegeld erpresst wird oder sie "geleaked" werden;

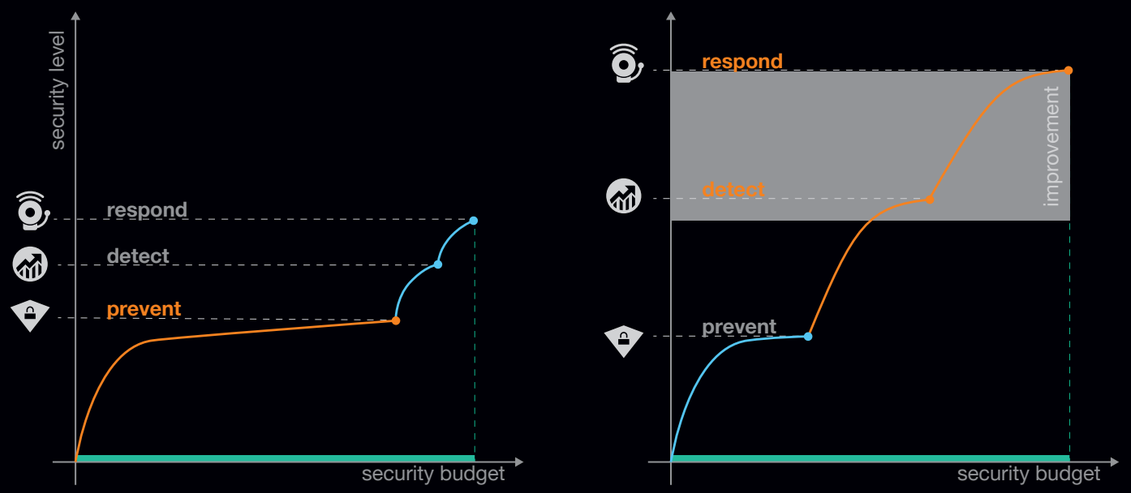
Unternehmen müssen akzeptieren, dass in ihre Infrastruktur eingedrungen wird, unabhängig davon, wie viel sie in präventive Technologien investieren. Sobald sie dies erkannt haben, müssen sie einen Plan haben, wie sie einen Angriff erkennen, wie sie die Auswirkungen begrenzen und wie sie so schnell und effektiv wie möglich darauf reagieren können. Dies ist der Bereich, in den sich die Investitionen laut unseren Prognosen im Laufe des Jahres 2020 verlagern werden.

Erkennen des Verhaltens

Wenn wir die Tatsache akzeptieren, dass wir unsere Fähigkeit zur Erkennung von Bedrohungen verbessern müssen, wie können wir dies umsetzen? Wir gehen davon aus, dass sich der Schwerpunkt auf die nur Log-basierte Erkennung verlagern wird, um auch die netzwerkbasierte und endpunktbasierte Erkennung mit einzubeziehen. Sie sollten eine Detection-Strategie wählen, die auf Ihre Umgebung und Ihre Anforderungen abgestimmt ist. Wenn Compliance-gesteuerte Erkennung am wichtigsten ist, dann könnten Logs das richtige Mittel sein. Wenn Sie eine schnelle Time-to-Value und erweiterte Detection und Response-Möglichkeit wünschen, dann ist der Endpoint das Richtige für Sie. Wenn Sie keine Sensoren an Ihren Endpunkten installieren können, dann sollten Sie über netzwerkbasierte Detection nachdenken. Wenn Sie hohe Anforderungen an die Detection stellen, benötigen Sie eine Kombination aus all dem oben genannten.

Es ist inzwischen allgemein bekannt, dass die Cybersecurity wirklich ein Thema für "Big Data" ist. Unabhängig davon, ob Sie Endpoint-Daten, Netzwerkdaten oder Protokolldaten analysieren. Um dieses Problem zu lösen, müssen Unternehmen ihre Investitionen in Technologien mit starken AI/ML-Implementierungen erhöhen, um damit die Analyse dieser riesigen Datenmengen zu unterstützen. Der Schlüssel zum Einsatz von AI/ML-Technologien liegt in der Erkenntnis, dass diese Technologien kein Allheilmittel sind. Um effektiv zu sein, muss es ein definiertes Problem geben, für das wir die Technologie als Werkzeug nutzen können - und nicht als Lösung. Gute AI/ML-Implementierungen können die Arbeit der Analytiker erheblich entlasten und sind, zusammen mit Orchestrierung und Automatisierung, in Zukunft die Schlüsselkomponenten für den Aufbau eines SOC.

Einen Teil des Budgets in Detection & Response zu investieren bringt mehr, als übermäßig große Summen allein für Prävention auszugeben



Response als Zusatzfunktion

Nun, da wir den Technologieansatz geklärt haben, wie geht es weiter? Sie benötigen Mitarbeiter und Prozesse, um die Analyse und Klassifizierung der Detection rund um die Uhr durchzuführen. Die meisten Unternehmen haben mit den Kosten und der Zeit zu kämpfen, dies selbst auf die Beine zu stellen. Daher kaufen sie dies als Dienstleistung (MDR), mit dem zusätzlichen Vorteil, dass sie auch rund um die Uhr eine Rückmeldung erhalten.

Bei jedem Security Incident ist die Höhe des Schadens umgekehrt proportional zu der Zeit, bis der Vorfall entdeckt wird. Um es auf den Punkt zu bringen: Je schneller Sie einen potenziellen Vorfall erkennen können, desto weniger Schaden entsteht.

Daher hängt das von einem Vorfall ausgehende Risiko davon ab, wie schnell Sie eine Bedrohung erkennen und darauf reagieren können. Aber die bloße Erkennung eines Vorfalls ist nur ein Teil von guter Security, Response und Recovery sind ebenso wichtig.

Im Jahr 2019 haben viele Kunden unsere Notfall-Hotline angerufen, um bei Zwischenfällen Hilfe zu erhalten. Wir gehen davon aus, dass die Kunden im Jahr 2020 beginnen werden, proaktiver zu werden und ihre internen Fähigkeiten zu analysieren, um schnell auf Bedrohungen reagieren zu können, und dies zusätzlich noch ergänzen werden durch ein Abonnement von vertrauenswürdigen Security Anbietern.

Alles beginnt mit Transparenz

Da die Budgets für Cybersecurity begrenzt sind, müssen die Investitionen mit Bedacht eingesetzt werden. Um die richtige Entscheidung treffen zu können, in welchen Bereich am sinnvollsten investiert werden soll, benötigt man Daten und Visibility. Daher glauben wir, dass sich die Investitionen in Zukunft auf diesen Bereich verlagern werden.

Hier sind einige Beispiele oder Bereiche, in denen wir eine verstärkte Nachfrage feststellen konnten.

Endpoint & Network Transparenz

Seit Jahrzehnten sind SIEM-Lösungen die primäre Methode zur Erkennung und Reaktion auf Bedrohungen. Die Implementierungen beanspruchen Zeit, Abstimmung und Wartung. Am Ende steht und fällt der Nutzen mit der Qualität der Daten, die zur Verfügung gestellt werden. Wir sind nach wie vor der Meinung, dass SIEM eine entscheidende Komponente im SOC-Werkzeugkasten ist, aber Sie können Ihre Wertschöpfung optimieren und Ihre Fähigkeiten zur Erkennung von Bedrohungen verbessern, indem Sie eine Endpoint- oder Netzwerk-basierte Detection einsetzen. Wir erkennen einen Trend, in diese beiden Technologien zu investieren. Ebenso wie Managed Service, für Kunden, die nicht über ein eigenes 24x7 CSIRT-Team verfügen.

SIEM für Transparenz bei Maschinen-Daten

Wir alle kennen den Ausdruck "Data is the new oil". Warum versuchen Sie also nicht, alle Daten, die Ihr Unternehmen täglich erstellt, zu nutzen, um datengestützte Entscheidungen zu treffen und Ihr Unternehmen effektiver zu steuern? Wir glauben, dass die bloße Sammlung von Logs für Security-Anwendungsfälle dazu übergehen wird, die gleichen (und zusätzliche) Daten für IT- und Betriebs-Use Cases zu nutzen.

Cloud Transparenz

Jeder bewegt sich in die Cloud, und die Devops-Teams bauen minütlich neue Umgebungen auf und ab. Gleichzeitig wissen wir, dass alle größeren Verstöße in Cloud-Infrastrukturen auf Fehlkonfigurationen oder Betriebspraktiken zurückzuführen sind. Wir glauben, dass die Technologie, die eine Verbindung zu Cloud-APIs herstellt, um Bestands- und Sicherheitsdaten zu extrahieren, für Ihr Security-Team sehr hilfreich sein wird, um eine gewisse Kontrolle über ihre Cloud-Infrastruktur zu erhalten und die Compliance-Arbeit zu erleichtern.

OT / ICS Transparenz

Bei Industrial Internet of Things (IIOT) und Industrie 4.0 dreht sich alles um die Verbindung von Maschinen mit anderen Maschinen und um die Optimierung und Produktivität in einer "smart factory".

Die Vorteile sind immens, aber auch die Herausforderungen sind beträchtlich. Eine große Herausforderung besteht darin, die Kluft zwischen OT-Experten und Security-Experten zu überbrücken, damit sie die Widrigkeiten in beiden Bereichen verstehen und gemeinsam sichere OT-Umgebungen aufbauen können. Ein guter Anfang ist es, sich einen Überblick darüber zu verschaffen, was mit diesen Netzwerken verbunden ist und wie sie kommunizieren. Dieses Wissen kann dann die Implementierung von Schutz- und Bedrohungserkennungslösungen zum Schutz dieser OT-Umgebungen ermöglichen.

Privileged Account Transparenz

Die Mehrzahl der Datenverstöße erfolgt durch die Verwendung von Konten, die eine hohe Berechtigungsstufe haben, um laterale Bewegungen und Datenexfiltration durchzuführen. Warum? Weil es einfach ist. Viele Organisationen haben keine Transparenz oder Kontrolle über all die hochsensiblen Konten. Eine gängige Schätzung lautet, dass die Anzahl der hoch eingestuften Konten etwa dreimal so hoch wie die Anzahl der normalen Benutzerkonten ist. Haben Sie die Kontrolle darüber, wer Zugriff auf diese Konten hat, wie Passwörter geteilt und rotiert werden und was die Personen tatsächlich tun, wenn sie als Administratoren angemeldet sind? Die Einsicht in Ihre aktuellen "privileged" Konten ist ein erster großer Schritt in Ihrem Plan, die Sicherheit eben dieser Konten zu implementieren.

Fazit: Wie geht es weiter?

Sobald Sie Einblick in Ihre Assets und Daten haben, müssen Investitionen in allen Bereichen der Prevention, Detection und Response getätigt werden. Wir prognostizieren:

Prevention wird von einem "Alles-oder-Nichts"-Ansatz zu einem risikobasierten Ansatz übergehen. Kritische Daten oder Mitarbeiter, die Zugang zu kritischen Daten haben, müssen weiterhin den erforderlichen Schutz erhalten.

Detection wird sich von 'Standard' auf kundenspezifische Detection verlagern. Generische Regeln in einem SIEM reichen nicht aus, um intelligente Gegner zu entdecken.

Response wird sich von der "Oops-Hilfe" zu einem proaktiven und geplanten Ansatz verlagern.

Die Kombination der eigenen Fähigkeiten mit der Nutzung externer Ressourcen ist der Weg in die Zukunft.

Viele Organisationen verfügen mittelfristig nicht über die erforderlichen Fähigkeiten in den Bereichen Detection und Response. Wir erwarten daher, dass der Markt für Managed Detection & Response-Services weiterhin deutlich wachsen wird.

120 Privatkliniken der Ramsay-Gruppe im Visier eines Cyber-Angriffs

Der Angriff verursachte einen IT-Blackout in Marseille, wurde aber durch Incident Response eingedämmt, bevor er sich ausbreiten konnte [t43].

SEP

Firefox 69 blockiert jetzt standardmäßig 3rd-Party-Tracking-Cookies und Cryptominers

Durch die standardmäßige Aktivierung eines verbesserten Trackingschutzes für alle Benutzer wird Mozilla automatisch beliebte Tracking-Cookies deaktivieren, wie Google Analytics und verhindert zusätzlich die Ausführung von JS-Cryptominers [t44].

Profil von Twitter-CEO Jack Dorsey gehackt

Twitter deaktiviert 'Twittern per SMS', nachdem Hacker mittels SIM-Swapping Dorseys Handynummer beansprucht hatten, die sie sich zuvor durch Social Engineering eines AT&T-Mitarbeiters verschafft hatten [t45].

Persönliche Daten von fast jedem ecuadorianischen Bürger geleaked

Der Geschäftsführer der IT-Beratungsfirma Novaestrat wurde verhaftet, nachdem persönliche Aufzeichnungen von so ziemlich der gesamten Bevölkerung auf einem öffentlichen und ungeschützten Elasticsearch-Server abgelegt wurden [t46].

Mehr als 16 Millionen Patientenakten aus 50 Ländern ungeschützt

Die Aufzeichnungen umfassen in erster Linie medizinische Bilder und Scans, z.B. Röntgenaufnahmen, MRTs, CT-Scans, zusammen mit persönlichen Daten wie Namen, Adressen und Sozialversicherungsnummern. Dies war kein Hack, sondern vielmehr die "normale" Art und Weise, wie solche Bilder jahrelang gespeichert wurden [t48].

Cryptomining-Botnet Smominru breitet sich weiter aus

Laut Untersuchungen von Guardicore infiziert die Malware jeden Monat bis zu 90.000 Kunden und nutzt die aus der berüchtigten WannaCry-Kampagne bekannte EternalBlue-Schwachstelle aus [t47].

OKT

Passwort nach 39 Jahren geknackt

Das Passwort gehört Ken Thompson, einem der Väter des ursprünglichen UNIX. Selbst im Jahr 2019 erwies sich das 8-stellige Passwort als unerwartet schwer zu knacken. Man fand heraus, dass es sich um einen kurzen Code für einen Schachzug handelte: Bauer von Dame 2 auf Dame 4, oder "p/q2q4!a" [t49].

GoSport und Courir GoSport von Ransomware getroffen

Die Vertriebsgruppen und Bekleidungseinzelhändler Go Sport und Courir werden Ende Oktober 2019 durch Ransomware lahmgelegt. Die Geschäfte müssen geschlossen werden und das Zahlungssystem ist für einige Zeit offline [t50].

Die Grand Cognac Agglomeration weigert sich, Lösegeld zu zahlen

400 Computer einschließlich Haupt- und Backup-Server werden per E-Mail infiziert, was zu einer Verschlüsselung von internen Arbeitsdokumenten aus 10 Jahren führt. Das geforderte Lösegeld beträgt €180.000 [t51].

M6, einer der größten Fernsehkanäle Frankreichs, von Ransomware betroffen

Frankreichs größter in Privatbesitz befindlicher Multimediakonzern ist von Ransomware betroffen. Dank modernster Cybersecurity können Ausfälle von Radio- und Fernsehkanälen verhindert werden [t52].

InfoTrax entdeckt laufenden Verstoß erst nachdem der Server keinen Speicherplatz mehr hatte

Anscheinend dauert der Verstoß seit 2014 an, wurde aber erst entdeckt, nachdem ein Archiv mit gestohlenen Daten, das die Hacker erstellt hatten, drohte, den Serverspeicherkapazität des Unternehmens zu überschreiten. InfoTrax bietet ERP-Lösungen an [t55].

Zahlungslösungs-Riese Edenred gesteht Cyberattacke ein

Das Unternehmen bietet 50 Millionen Kunden weltweit Lösungen für Arbeitnehmerleistungen, Fuhrpark und Mobilität sowie für Firmenzahlungen. Aufgrund der schnellen Reaktion konnten die Auswirkungen relativ begrenzt werden [t54].

Krankenhaus in Rouen wendet sich nach Cyberattacke Stift und Papier zu

Schnelles Handeln der französischen Behörde für Cyberkriminalität ANSSI trägt dazu bei, das Ausmaß des Ransomware-Ausbruchs einzudämmen und die Systeme schnell zurückzubringen [t53].

NOV

Datenleck bei T-Mobile US

Angreifer waren in der Lage, die persönlichen Daten von über einer Million Kunden zu erhalten. Offenbar waren Finanzinformationen und Passwortdaten nicht betroffen [t56].

DEZ

Neu entdeckter Fehler ermöglicht Angreifern, verschlüsselte VPN-Verbindungen zu kapern

CVE-2019-14899 betrifft die meisten Linux- und Unix-ähnlichen Betriebssysteme, einschließlich FreeBSD, OpenBSD, macOS, iOS und Android. Es könnte entfernten Netzwerk-Angreifern erlauben, verschlüsselte VPN-Verbindungen auszuspionieren (und sie zu manipulieren) [t57].

Snatch-Ransomware startet Windows im abgesicherten Modus neu, um den Virenschutz zu umgehen

Die Ransomware verwendet einen manipulierten Windows-Registrierungsschlüssel, um einen Dienst zu planen, der im abgesicherten Modus startet und von dort aus die Verschlüsselung ausführt. Snatch zielt speziell auf Unternehmen und Regierungseinrichtungen ab [t58].

Zusammenfassung:

Was haben wir gelernt?

Etienne Greef
CTO
Orange Cyberdefense

Es ist immer eine Herausforderung, nach so vielen interessanten Fakten und Meinungen eine Schlussfolgerung zu schreiben. Deshalb werde ich versuchen, die meiner Meinung nach wichtigsten Erkenntnisse aus diesem Security Navigator hervorzuheben.

Zu Beginn möchte ich auf das Grundprinzip des Digital Trust eingehen. Es ist ein Fakt, dass wir in einer sehr vernetzten Welt leben. Wir haben in jedem einzelnen Aspekt unseres Lebens zahlreiche Interaktionen mit digitalen und vernetzten Systemen. Diese Systeme machen unser Leben einfacher und verbessern unsere Lebensqualität erheblich. Aber mit den Vorteilen, kommen auch Nachteile. Als Verbraucher sind unsere Daten, Entscheidungen, Verhaltensweisen und Interaktionen mit anderen zu einer Ware geworden, die im Guten und leider auch im Schlechten verwendet werden kann. Ich denke nicht, dass die meisten von uns eine bewusste Entscheidung getroffen haben, freien Zugang zu unseren persönlichen Daten und damit zu unserem Leben zu gewähren, als wir anfingen, die verschiedenen Systeme zu nutzen und mit ihnen zu interagieren. Mit anderen Worten, als wir anfingen, die Vorteile der Technologie zu genießen, haben wir die potenziellen Nachteile nicht vollständig in Betracht gezogen. Wie dieser Bericht so anschaulich illustriert, werden unsere Daten oft kompromittiert, gehandelt und genutzt auf eine Art und Weise, mit der wir nie gerechnet hätten.

Ich spreche mich nicht dafür aus, keine Technologie mehr zu verwenden, aber ich glaube, dass Unternehmen einen Gang zulegen und die Verantwortung für die Daten übernehmen müssen, die wir ihnen anvertrauen. Ich glaube, dass die heutige Cybersecurity-Industrie ihr Versprechen, Vertrauen zu gewährleisten, nicht einhält. Trotz der Tatsache, dass die Ausgaben steigen, erleben wir immer häufiger immer größere Sicherheitsverstöße. In gewisser Weise liegt eine gewisse Müdigkeit diesbezüglich vor, denn die meisten Menschen zucken bei den letzten Berichten von Vorfällen fast mit den Schultern.

Der Nachrichtenzyklus wird von großen Sicherheitslücken beherrscht, aber die richtigen Lehren werden daraus oft nicht gezogen. Unsere Branche wird von der Technologie beherrscht, und die Technologieanbieter bieten immer mehr Lösungen an, um im Wesentlichen dasselbe Problem zu lösen. Meiner Meinung nach liegt der Schwerpunkt zu wenig auf dem Risikoverständnis, der Suche nach potenziellen Lücken und dem Aufbau einer robusten Response- und Recovery-Fähigkeit.

Um die Situation aus präventiver Sicht zu verbessern, möchte ich mich auf vier grundlegende Bereiche konzentrieren, Bereiche, die im gesamten Bericht diskutiert worden sind.

1 Menschliches Verhalten ändern

Dies ist oft der Teil der Cybersecurity, in den am wenigsten investiert wird.

Cyberdefense beginnt und endet bei unseren Benutzern. Unsere Benutzer werden oft als das schwächste Glied wahrgenommen, aber sie können unser stärkster Verbündeter sein, indem sie als intelligente menschliche Sensoren fungieren. Wenn es auch nur einen einzigen Ratschlag gibt, den ich dem typischen CISO geben würde, dann den, seine User aufzuklären und zu befähigen und sie nicht länger als Opfer zu betrachten.

2 Fokus auf Authentifizierung und Autorisierung

Angesichts der Zahl der kompromittierten Benutzerpasswörter, die der Hälfte der Weltbevölkerung entspricht, ist klar, dass die alleinige Verwendung von Passwörtern einfach nicht stark genug ist.

Die Authentifizierung sollte ein Muss sein und ebenso transparent und einfach zu handhaben sein wie Passwörter. Ich glaube, es ist an der Zeit, Passwörter abzuschaffen. Über die Passwörter hinaus ist es auch wichtig, sich auf die Autorisierung zu konzentrieren und das Prinzip der geringsten Privilegien in die Praxis umzusetzen. Unsere ethischen Hacker lieben ein Benutzerkonto mit Admin-Privileg oder ein Admin-Konto mit dem gleichen Passwort wie ein Benutzer.

3 Barrieren innerhalb von Netzwerken errichten

Eines der grundlegendsten Prinzipien der Netzwerksicherheit ist das der Zonen des Vertrauens. Eine Zone des Vertrauens ist im Grunde die Gruppierung von Geräten oder Daten mit einem ähnlichen "Level of Trust". Viele Unternehmen haben nur ein einziges Level mit wenigen Barrieren innerhalb des Netzwerks. Was bei vielen Verstößen überrascht, ist nicht die Tatsache, dass Unternehmen Verstöße verzeichnen.

Es ist die Tatsache, dass Hacker, sobald sie einmal eingedrungen sind, frei innerhalb des Zielnetzwerks umherwandern können.

4 Ihre Angriffsfläche und Schwachstellen verstehen

Hacking ist fast nie so weit fortgeschritten, wie die Presse uns glauben machen will. In den meisten Fällen sind die ausgenutzten Schwachstellen alt und wohlverstanden. Vieles deutet darauf hin, dass das Durchschnittsalter einer bei größeren Angriffen ausgenutzten Schwachstelle bei 90 Tagen liegt. Bei vielen der jüngsten Angriffe brauchten die Schurken nicht einmal eine Schwachstelle auszunutzen. Alles, was sie tun mussten, war eine Datenbank von einem öffentlichen Server ohne Passwort herunterzuladen. Wenn Unternehmen genauso viel Zeit damit verbringen würden, ihre Angriffsfläche und Schwachstellen zu verstehen, wie sie versuchen, den neuesten technologischen Security-Trend umzusetzen, würde unser Bericht viel kürzer ausfallen. Ein gut strukturiertes Programm für das Management von Schwachstellen in Verbindung mit einem detaillierten Verständnis Ihrer Umgebung und des Ortes, an dem die Daten liegen, wird das Niveau Ihrer Sicherheit exponentiell erhöhen.

Wir leben mit Sicherheit in interessanten Zeiten mit der COVID-19-Pandemie, die eine beispiellose Geschäftstransformation bewirkt. Das Tempo der Transformation war, gelinde gesagt, erstaunlich, da die meisten Unternehmen ihre Arbeitsweise innerhalb weniger Wochen vollständig verändert haben. Offensichtlich hat diese Transformation einige neue Herausforderungen in Bezug auf die Sicherheit geschaffen. Aber man könnte argumentieren, dass die Herausforderungen nicht wirklich neu sind. Fernzugriff ist seit geraumer Zeit Realität. Die neue massive Verlagerung auf Homeoffice- und Cloud-Infrastruktur hat die Nachfrage nach Transparenz nur noch verstärkt, da der Perimeter jetzt wirklich bei jedem Mitarbeiter zu Hause ist.

Wenn der klassische Perimeter wegfällt, müssen intelligente Lösungen implementiert werden, um Bedrohungen zu verhindern, zu erkennen und darauf zu reagieren. Es ist auch wichtig zu überlegen, was passiert, wenn eine Menge von Geräten ins Büro zurückkehren, die längere Zeit nicht den Schutz der Unternehmenssicherheit genossen haben und wieder in unsere Unternehmensnetzwerke aufgenommen werden müssen.

Abschließend möchte ich sagen, dass sich Cyberkriminalität derzeit auszahlt und zwar recht gut. Wie in dem Bericht erörtert, erhalten Hacker häufig Lösegeld, insbesondere wenn eine Cyberversicherung besteht. Hacker, die sechsstellige Belohnungen für das Hacken erhalten, nähren das kriminelle Ökosystem und das wird höchstwahrscheinlich zu einer deutlichen Zunahme der Hacking-Aktivitäten führen. In meinen Augen ist dies die größte Einzelveränderung in unserer Cybersicherheitswelt im Jahr 2019. Kriminelle können ihr Handwerk mit immer ausgefeilteren Werkzeugen monetarisieren, die häufig sogar von Regierungen entwickelt werden. Das ist besorgniserregend und bedeutet, dass Unternehmen davon ausgehen müssen, dass sie irgendwann zum Ziel werden. Wie Stefan Lager sagte, müssen wir uns genauso auf das Verständnis unseres Risikos, das Erkennen von Problemen, die Reaktion und die Wiederherstellung konzentrieren, wie auf den Schutz unserer Assets.

2020 Timeline ▸

Mitwirkende, Quellen und Links

Quellen

Dieser Bericht hätte nicht ohne die harte Arbeit vieler Forscher, Journalisten und Organisationen auf der ganzen Welt erstellt werden können. Wir haben dankend ihre Online-Publikationen als Referenz oder Kontext verwendet.

Statistiken and Zahlen

Alle Statistiken ohne explizite Quellenangabe stammen aus den CyberSOCs von Orange Cyberdefense

Story: Die Fondation du Patrimoine und der Notre-Dame Brand

[1.1] https://www.zdnet.fr/actualites/notre-dame-de-paris-elan-de-solidarite-et-arnaques-en-tout-genre-39892077.htm

[1.2] Letter dated July 12, 2019 from Mr. Guillaume Poitrinal, President of the Fondation du Patrimoine to Orange Cyberdefense

CyberSOC Statistiken

[2.3] https://coinmarketcap.com/currencies/monero/

[2.4] https://coinmarketcap.com/currencies/ethereum/

[2.5] https://coinmarketcap.com/currencies/litecoin/

[2.6] https://coinmarketcap.com/currencies/bitcoin/

[2.7] https://www.biznesstransform.com/transforming-the-food-and-beverage-industry-with-digital-technologies/

Datenlecks überall

[4.1] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[4.2] https://www.lowyat.net/2019/177033/over-1-million-uitm-students-and-alumni-personal-details-leaked-online

[4.3] https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html

[4.4] https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

[4.5] https://thehackernews.com/2019/02/data-breach-website.html

[4.6] https://thehackernews.com/2019/02/data-breach-sale-darkweb.html

[4.7] https://www.todayonline.com/singapore/personal-data-808000-blood-donors-compromised-nine-weeks-hsa-lodges-police-report

[4.8] https://thehackernews.com/2019/03/data-breach-security.html

[4.9] https://www.upguard.com/breaches/facebook-user-data-leak

[4.10] https://www.businessinsider.com/facebook-uploaded-1-5-million-users-email-contacts-without-permission-2019-4

[4.11] https://economictimes.indiatimes.com/tech/internet/data-breach-at-justdial-leaks-100-million-user-details/articleshow/68930607.cms

[4.12] https://www.vpnmentor.com/blog/report-millions-homes-exposed/

[4.13] https://www.analyticsindiamag.com/data-breach-truecaller-exposes-indian-users-data-shows-cracks-in-cyber-security-infrastructure/

[4.14] https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

[4.15] https://www.cisomag.com/nearly-140-million-user-data-leaked-in-canva-hack/

[4.16] https://finance.nine.com.au/business-news/westpac-data-breach-100000-australian-customers-at-risk/84c91581-90b6-464e-9137-a2d973492614

[4.17] https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach

[4.18] https://www.publishedreporter.com/2019/06/05/nearly-12-million-quest-diagnostics-patients-medical-info-exposed-in-new-data-breach/

[4.19] https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297

[4.20] https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-steal-millions-of-bulgarians-financial-records-tax-agency-idUSKCN1UB0MA

[4.21] https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

[4.22] https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/

[4.23] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

[4.24] https://www.vpnmentor.com/blog/report-ecuador-leak/

[4.25] https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure

[4.26] https://japan.cnet.com/article/35143123/

[4.27] https://techcrunch.com/2019/09/26/doordash-data-breach/

[4.28] https://venturebeat.com/2019/09/30/words-with-friends-player-data-allegedly-stolen-for-218-million-users/

[4.29] https://www.worldometers.info/world-population/

[4.30] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[4.31] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Die PKI und Digital Trust

[6.1] https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-certification-authorities

[6.2] https://www.bloomberg.com/profiles/companies/108453Z:SS-addtrust-ab

[6.3] http://web.archive.org/web/20110128085641/http://www.addtrust.com/

[6.4] https://en.wikipedia.org/wiki/Certificate_authority

[6.5] https://www.xolphin.com/support/Rootcertificates/Phasing_out_Addtrust_External_CA_Root_certificate

Security Prognosen

[7.1] https://towardsdatascience.com/google-has-cracked-quantum-supremacy-cd70c79a774b

Timeline

[t1] https://www.avanan.com/resources/zwasp-microsoft-office-365-phishing-vulnerability

[t2] https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support

[t3] https://www.safetydetectives.com/blog/major-security-breach-discovered-affecting-nearly-half-of-all-airline-travelers-worldwide/

[t4] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[t5] https://www.reuters.com/article/us-altran-tech-cyber/frances-altran-tech-says-it-was-hit-by-cyber-attack-idUSKCN1PM0IJ

[t6] https://www.carbonblack.com/2019/01/24/carbon-black-tau-threatsight-analysis-gandcrab-and-ursnif-campaign/

[t7] https://www.reuters.com/article/us-airbus-cyberattack-report/hackers-tried-to-steal-airbus-secrets-via-contractors-afp-idUSKBN1WB0U9

[t8] https://thehackernews.com/2019/02/cryptocurrency-exchange-exit-scam.html

[t9] https://blog.zimperium.com/dont-give-me-a-brake-xiaomi-scooter-hack-enables-dangerous-accelerations-and-stops-for-unsuspecting-riders/

[t10] https://thehackernews.com/2019/02/vfemail-cyber-attack.html

[t11] https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/ , https://thehackernews.com/2019/02/data-breach-sale-darkweb.html

[t12] https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20190303005031

[t13] https://blog.mozilla.org/blog/2019/03/12/introducing-firefox-send-providing-free-file-transfers-while-keeping-your-personal-information-private/

[t14] https://thehackernews.com/2019/03/data-breach-security.html

[t15] https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

[t16] https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-producer-hydro-hit-by-cyber-attack-shuts-some-plants-idUSKCN1R00NJ

[t17] https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

[t18] https://cafe.bithumb.com/view/board-contents/1640037

[t19] https://www.upguard.com/breaches/facebook-user-data-leak

[t20] https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN-1RG0NN

[t21] https://securelist.com/project-tajmahal/90240/

[t22] https://medium.com/@fs0c131y/tchap-the-super-not-secure-app-of-the-french-government-84b31517d144

[t23] https://blog.malwarebytes.com/cybercrime/2019/04/electrum-ddos-botnet-reaches-152000-infected-hosts/

[t24] https://vaaju.com/franceeng/fleury-michon-stopped-production-for-five-days-due-to-a-computer-virus/

[t25] https://www.vpnmentor.com/blog/report-millions-homes-exposed/

[t26] https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

[t27] https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html

[t28] https://www.lemondeinformatique.fr/actualites/lire-le-site-des-aeroports-de-lyon-cible-par-une-cyberattaque-75489.html

[t29] https://morphuslabs.com/goldbrute-botnet-brute-forcing-1-5-million-rdp-servers-371f219ec37d

[t30] https://labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind/

[t31] https://moneyandpayments.simonl.org/2019/06/perspectives-on-ca-libra-1-first-we-get.html

[t32] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

[t33] https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

[t34] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

[t35] https://thehackernews.com/2019/07/ransomware-nas-devices.html

[t36] https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/

[t37] https://twitter.com/CityPowerJhb/status/1154277777950093313

[t38] https://research.checkpoint.com/say-cheese-ransomware-ing-a-dslr-camera/

[t39] https://www.ecb.europa.eu/press/pr/date/2019/html/ecb.pr190815~b1662300c5.en.html

[t40] https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/

[t41] https://thehackernews.com/2019/08/dds-safe-dental-ransomware-attack.html

[t42] https://www.theregister.co.uk/2019/08/21/kazakstan_snooping_blockade/

[t43] https://www.tellerreport.com/life/2019-08-13---the-120-hospitals-of-the-ramsay-health-group-in-france-victims-of-a-cyber-attack-.rJQ3yHqg4r.html

[t44] https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

[t45] https://thehackernews.com/2019/09/tweet-via-sms-text-message-hacking.html

[t46] https://www.vpnmentor.com/blog/report-ecuador-leak/

[t47] https://www.guardicore.com/2019/09/smominru-botnet-attack-breaches-windows-machines-using-eternalblue-exploit

[t48] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

[t49] https://thehackernews.com/2019/10/unix-bsd-password-cracked.html

[t50] https://www.lemondeinformatique.fr/actualites/lire-go-sport-et-courir-victimes-d-un-ransomware-77403.html

[t51] http://www.leparisien.fr/societe/cyberattaque-l-agglomeration-grand-cognac-refuse-de-payer-la-rancon-31-10-2019-8183676.php

[t52] https://www.zdnet.com/article/m6-one-of-frances-biggest-tv-channels-hit-by-ransomware/

[t53] https://www.bbc.com/news/technology-50503841

[t54] https://www.bleepingcomputer.com/news/security/edenred-payment-solutions-giant-announces-malware-incident/

[t55] https://thehackernews.com/2019/11/hacking-file-storage.html

[t56] https://www.techradar.com/news/over-a-million-t-mobile-customers-hit-in-data-breach

[t57] https://thehackernews.com/2019/12/linux-vpn-hacking.html

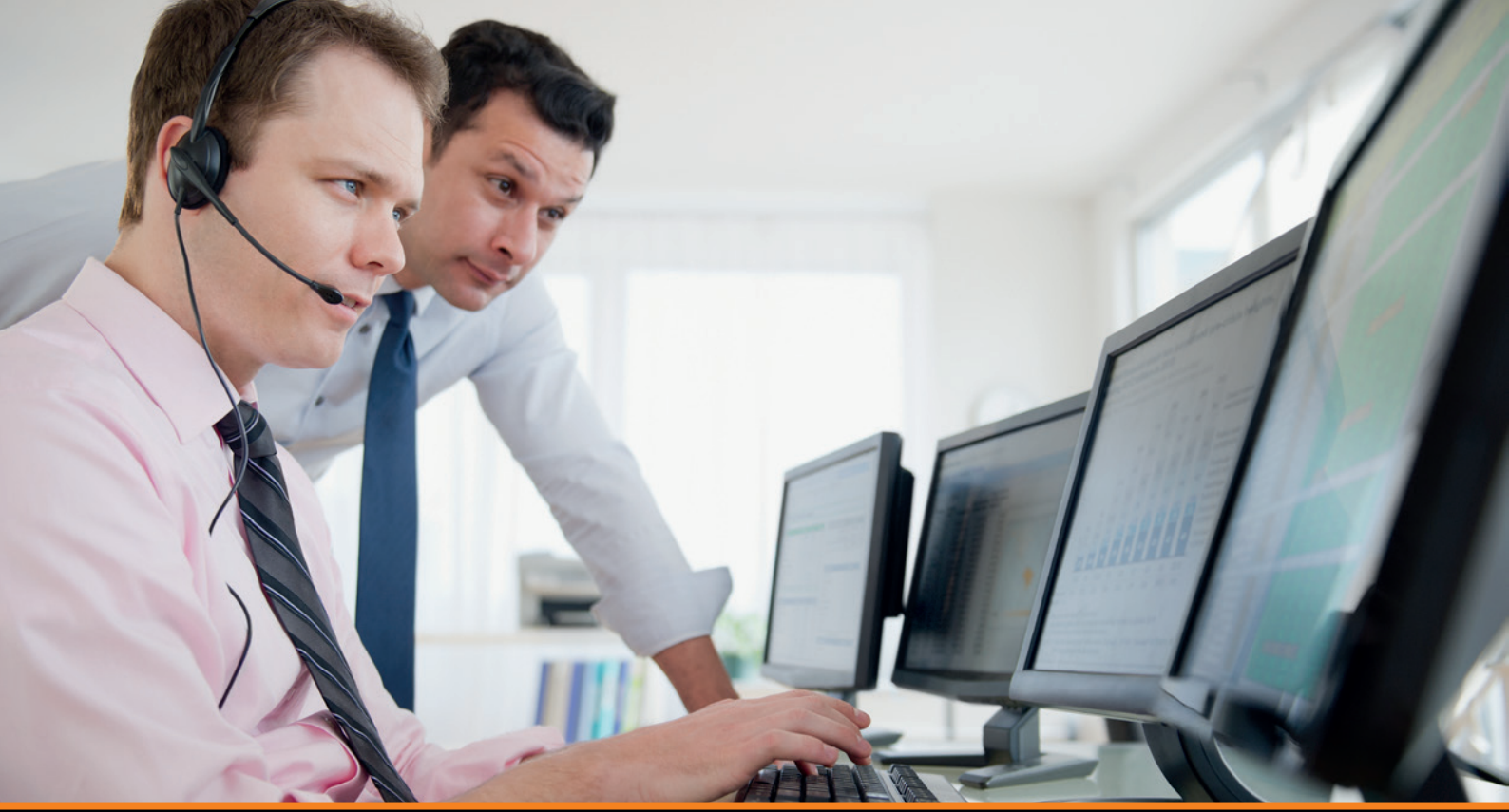
[t58] https://www.zdnet.com/article/snatch-ransomware-reboots-pcs-in-windows-safe-mode-to-bypass-antivirus-apps/

[t59] https://security.googleblog.com/2019/12/announcing-updates-to-our-patch-rewards.html

Haftungsausschluss

In Notfällen können Sie unser CSIRT-Team über die Hotline Ihres Landes rund um die Uhr erreichen! Finden Sie die Hotline Ihres Landes unter **orangecyberdefense.com!**

Ein ganz besonderer Dank gilt allen Cyber-Huntern, Analysten und Ingenieuren in unseren SOCs.



Warum Orange Cyberdefense?

Cybersecurity Spezialisten
Orange Cyberdefense ist auf Cyber-Security Services und -Lösungen spezialisiert und kann auf eine 25-jährige Erfolgsgeschichte bei der Erbringung von Managed Services für einige der größten Unternehmen der Welt zurückblicken.

Hervorragende Expertise
Unsere Services werden von unseren 10 CyberSOCs und 16 SOCs weltweit erbracht, die einen sofortigen 24x7x365-Zugang zu Spezialisten bieten, die sich mit Vorfällen befassen und eine ständige Verfügbarkeit gewährleisten.

Vendor Insights
Unsere enge Partnerschaft mit zahlreichen Anbietern bietet einen hervorragenden Zugang zu deren technischen Experten und Produkt-Roadmaps – so bleiben unsere CyberSOCs immer einen Schritt voraus.

Umfassende Security Insights
Die "Greater Intelligence"-Plattform von Orange Cyberdefense verarbeitet über 50 Milliarden Ereignisse pro Monat und ermöglicht uns so einen beispiellosen Zugang zu aktuellen und aufkommenden Bedrohungen. Unsere Elite-Consulting Team steht an vorderster Front der Cyber-Security – und gibt Einblick in kriminelle Denkweisen. Wir verwenden diese Informationen, um sicherzustellen, dass unsere Kunden so sicher wie möglich sind.

www.orangecyberdefense.com