

EIN BLICK IN DIE KRISTALLKUGEL: 2021 - SICHERHEITSTRENDS UND PROGNOSEN FÜR DAS KOMMENDE JAHR

Das Jahr 2020 begann buchstäblich mit einem Paukenschlag: Der iranische General Soleimani wurde, nicht einmal eine Woche nach Jahresbeginn, durch einen gezielten Raketenangriff getötet. Der Vorfall hatte unmittelbare Auswirkungen im Cyberspace. Darunter simple Website-Defacements seitens weniger wichtiger Akteure, die sich ideologisch dem Iran verbunden fühlten, aber er löste auch Sorge hinsichtlich weiterer Cyber-Eskalationen aus.

Dann fegten COVID-19 und die globalen Black Lives Matter-Proteste das Ereignis von der Agenda. Als die Welt schlagartig mit kompletten Belegschaften zum Remote Working übergehen musste, nutzten Angreifer primär dieselben Tools wie sonst auch: DDoS, Phishing, Ransomware und die übrigen üblichen Verdächtigen. Bei Cybereason haben wir Hunderten von Kunden gezeigt, was "elastische Sicherheit" bedeutet, indem wir insbesondere Dienste zum Schutz von im Homeoffice arbeitender Belegschaften so schnell wie möglich ausgebaut haben. Dazu kamen neue Funktionen speziell für die Sicherheit mobiler Geräte wie XDR.

Die Verteidiger fühlten sich zeitweise ins Jahr 2000 zurückversetzt, als grundlegende Konnektivitätsprobleme eine große Rolle gespielt haben: Helpdesk-Tickets mit Passwort- und VPN-Problemen, einbrechende Produktivität und die aufkeimende Hoffnung auf eine "neue Normalität". In der Sicherheitsbranche waren wir dabei, als für viele Unternehmen existenzielle Fragen diskutiert wurden: Die Begriffe Vertraulichkeit, Integrität und Verfügbarkeit hörte man in den (virtuellen) Vorstandsetagen so oft wie seit Jahren nicht mehr.

Für die einen war es eine Chance, die Lücken zwischen Sicherheit und geschäftlichen Anforderungen zu schließen. Für die anderen war es nur ein kurzes Aufflackern der Aufmerksamkeit. Die Verteidiger lernten, wieder Hand in Hand mit der IT zu arbeiten, um notwendige Services zu gewährleisten und die Basis für eine neue Normalität zu schaffen.

Die Angreifer waren allerdings auch nicht untätig. Covid-19 wurde rasch zum neuen „Watering Hole“ für so gut wie jeden. Praktisch sofort tauchten entsprechende mobile Bedrohungen auf. Covid-19 war der unwiderstehliche Clickbait, und man konnte so ziemlich alles beobachten - von Smishing bis hin zu einer gefälschten WHO-App und dem heimtückischen Eventbot. Wir beobachten schon seit Jahren wie sich Fileless Malware weiterentwickelt, während demgegenüber die Entwicklung bei Ransomware eher rückläufig ist. Sind fortschrittliche Angreifer die heimlichen Infiltratoren, dann ist Ransomware der Überfall und ein Schlag ins Gesicht der Opfer – um im Bild zu bleiben.

Aktuell beobachten wir das Aufkommen von RansomOps – also die Konvergenz von langsam und geduldig ausgeführten böswilligen Operationen gepaart mit der Power einer gut ausgearbeiteten Ransomware als Payload. Dabei gerieten diejenigen ins Fadenkreuz, die am ehesten gezwungen sind zu zahlen: das Gesundheitswesen, kritische Infrastrukturen, ganze Städte, die darum kämpfen, ihre Service-Infrastruktur aufrechtzuerhalten und sogar Vertriebsunternehmen für Hochprozentiges.

2020 wurde zum eigenständigen Begriff und Thema zahlreicher Meme. Trotzdem haben wir die größte Remote-Belegschaft überhaupt mobilisiert, die Geschäftstätigkeit katalysiert und es sogar geschafft, weniger fossile Brennstoffe zu verbrauchen. Angesichts dessen stellt sich nun die Frage, was hält 2021 für uns alle in einer globalisierten, vernetzten und einer Welt des „new normal“ bereit?

RISIKO HOMEOFFICE - ARBEITEN VON ZU HAUSE IM JAHR 2021

Von Yossi Naar, Chief Visionary Officer, Mitgründer von Cybereason

Einer der großen Veränderungen weltweit war der schnelle und umfassende Wechsel zur Arbeit vom Homeoffice aus aufgrund von Covid-19.

Diese Veränderung ging für die IT-Abteilungen mit reichlich Herausforderungen einher. Herausforderungen, die Hacker ihrerseits nicht zögerten für sich auszunutzen.

Davon können wir 2021 mehr erwarten. Jedenfalls dann, wenn uns Remote Working erhalten bleibt und Unternehmen ihre physischen Geschäftsräumlichkeiten dauerhaft verkleinern. Und wenn sie ihren Mitarbeitern die Flexibilität geben, weiterhin von zu Hause aus zu arbeiten.

Die häusliche Umgebung war für die Sicherheitsbranche schon immer ein Grund zur Sorge. Heimische Geräte werden selten gepatched, nicht ordnungsgemäß verwaltet, und sie lassen sich für Angriffe ausnutzen, ohne dass es jemand bemerkt.

Heimische Router sind besonders anfällig, weil Patches nicht regelmäßig eingespielt werden. Dazu kommt, dass Schwachstellen bei älteren Geräten nicht immer gefixt werden, man sie also gar nicht patchen kann.

Eine ohnehin problematische häusliche Umgebung, in der Geräte oft von mehreren Familienmitgliedern benutzt werden, und der schnelle Wandel ließen insgesamt nur wenig Zeit, sich vorzubereiten. Hacker haben die Situation weidlich ausgenutzt. Sie verwendeten Phishing-Angriffe und bekannte Exploits, um in Remote-Umgebungen einzudringen und sich dort einzunisten.

Unternehmen, die sich bei der Home-Office-Umstellung Zeit gelassen haben und die weitgehend dem traditionellen Perimeterschutz vertrauen, bleiben besonders anfällig, wenn ganze Belegschaften remote arbeiten. Eine Reihe von Unternehmen hatte noch gar nicht die Zeit, ihre Netzwerkumgebung vorzubereiten und entsprechend der neuen Realität aufzurüsten.

Aber es gibt auch Positives zu vermelden. Wir sehen Fortschritte bei der Einführung von Zero Trust und beobachten einen grundlegenden Wandel in der Sichtweise der IT auf Cloud-Workloads sowie bei der Remote-Überwachung von Geräten.

Es herrscht Konsens darüber, dass Remote Working gekommen ist, um zu bleiben - und diese Einsicht hat einen Paradigmenwechsel im IT-Management und hinsichtlich von Sicherheitsmaßnahmen gefördert und beschleunigt.

Viele Geräte in einem typischen Heimnetzwerk wie Drucker, Router und neuere, tendenziell schlecht geschützte IoT-Geräte, bieten Hackern perfekte Möglichkeiten, dauerhaft in einer lokalen Umgebung dieser Art Fuß zu fassen. Zerologon ist ein Beispiel wie neu auftretende Sicherheitslücken benutzt werden, um nicht gepatchte Netzwerke zu übernehmen, sich auszubreiten und dauerhaft einzunisten.



Das Risiko von Kreuzinfektionen zwischen verschiedenen Umgebungen zwingt uns dazu, den Einsatz von endpunktbasierten Schutzmaßnahmen zu beschleunigen, um zeitnah zu erkennen, was tatsächlich vorgeht. Hacker mussten sich ebenfalls anpassen. Hatten sie bisher überwiegend Unternehmen im Visier, werden jetzt zunehmend heimische Netze zum lukrativen Einstiegspunkt. Ja, auch die Angreifer brauchten Zeit, um sich an die neue Situation anzupassen. Aber sie tun das sehr schnell.

2021 kann zu einem transformativen Jahr für die globale Cybersicherheit werden - Verteidiger und Angreifer agieren jetzt auf ein und demselben Schlachtfeld. Die Illusion eines grundsätzlich sicheren internen Unternehmensnetzwerks existiert nicht mehr. Diese Verschiebung ist aber eine positive Entwicklung, denn sie fördert ein gesünderes, sichereres Verständnis dessen worum es tatsächlich geht, nicht zuletzt in einer sicheren Home-Office-Umgebung.

Home-Office-Risiken 2021 beseitigen

Virtuelle private Netzwerke, kurz VPNs, sind für viele Unternehmen so etwas wie eine Lebensader, weil sie verschlüsselte Netzwerke ins heimische Office ausdehnen. Um die Risiken zu minimieren, ist es wichtig, in dieser Phase die Integrität der Endpunkte zu überprüfen und starke Authentifizierung zu verwenden, wenn das VPN eingerichtet und aktiv ist.

Sobald das VPN gesichert ist, sollten Sie Ihre Aufmerksamkeit auf mobile Endgeräte richten. Sie sind die am weitesten verbreitete und allgegenwärtige Plattform in unserem Privatleben. Mitarbeiter, die sich mit neuen Geräten und Anwendungen vertraut machen müssen, werden noch häufiger als sonst zum Handy greifen. Einfach, weil es ihnen so vertraut ist. Die meisten Unternehmen haben Richtlinien festgelegt, was Mitarbeiter mit ihren Mobiltelefonen tun dürfen und was nicht. Legen Sie unbedingt solche Richtlinien fest, wenn Sie es nicht bereits getan haben. Beugen Sie vor allem mobilen Bedrohungen vor, bevor Sie sich mit anderen Geräten befassen.

Als nächstes sollten Sie Ihre Mitarbeiter darüber aufklären, wie Informationen zur Waffe werden. Die baldige Verfügbarkeit von Covid-19-Impfstoffen gibt Hackern weiterhin Gelegenheit, menschliche Schwächen auszunutzen. Als ein Großteil Nordamerikas im März und April in einen Lockdown ging, entwickelten Hacker eine bösartige mobile App, die sich als eine legitime App der Weltgesundheitsorganisation tarnte. Wer etwa einer Risikogruppe angehört, ist leicht geneigt diese bösartige App mit einer echten WHO-App zu verwechseln. Man kann definitiv davon ausgehen, dass Hacker neuartige Scams und betrügerische Apps entwickeln werden, die sich auf die veränderten menschlichen Bedürfnisse einstellen.

Der physische Standort der Mitarbeiter wird 2021 weiterhin von Bedeutung sein. Zwischen Routern, Druckern, Maschinen, Geräten, Spielekonsolen und Heimautomation besteht in einem durchschnittlichen Haushalt ein komplexeres und vielfältigeres Kommunikations- und Verarbeitungssystem als in manch einer kleinen Firma. Mitarbeiter führen möglicherweise Telefonkonferenzen in Hörweite von Familienmitgliedern oder sogar Mitarbeitern anderer Unternehmen durch. Man sollte nichts als selbstverständlich betrachten, wenn es um die Privatsphäre der Mitarbeiter zu Hause geht.

Sollten Mitarbeiter bei Besprechungen die Kameras ein- oder ausschalten? Sollten sie Kopfhörer tragen? Sollten sie sich Notizen auf Papier machen oder doch lieber digitale Apps nutzen? Welche Kommunikationsanwendungen sind akzeptabel? Was passiert, wenn andere den Raum betreten, Notizen zu Gesicht bekommen oder Gespräche mithören? Diese Fragen mögen trivial erscheinen, aber man sollte sie im Voraus klären.

Und vor allem: Hören Sie gut zu, wenn etwas nicht funktioniert und ändern Sie es.

MEHR CYBER-BEDROHUNGEN GEGEN KLEINE UND MITTLERE UNTERNEHMEN IM JAHR 2021

Von Israel Barak, Chief Information Security Officer, Cybereason

Kleine und mittelständische Unternehmen (KMUs) sind nicht selten "Gelegenheitsopfer" – meist handelt es sich um ungezielte Kampagnen, die zufällig Assets eines Unternehmens wie E-Mails oder IP-Adressen treffen.

Ein verwundbarer Perimeter führt oft zu einer Sicherheitsverletzung, die schwerwiegende geschäftliche Auswirkungen haben und eine Ransomware-Infektion oder einen Denial-of-Service nach sich ziehen kann.

Cyber-Kriminelle greifen KMUs meist wegen des Wertes der von ihnen bereitgestellten Daten oder Dienste (z. B. Kreditkarteninformationen) an. Vor allem, wenn Angreifer davon ausgehen, dass der Wert der kompromittierten Daten den Aufwand rechtfertigt, ein scheinbar unzureichend geschütztes Ziel zu kompromittieren.

KMUs, die Managed oder Professional Services für größere Unternehmen anbieten, sind oft so etwas wie "Etappenziele" - sie fungieren als Ausgangspunkt, um einem Angreifer Zugang zu Daten oder Systemen der betreffenden Kunden zu verschaffen.

Die größten Sicherheitsrisiken für KMUs 2021:

- Mobile Endgeräte
- Die beschleunigte Einführung von Cloud-Diensten
- Eine wachsende Zahl von Angriffen, die sich gegen Anbieter von Managed/Professional Services richtet

Mobile Technologien, Bring Your Own Device und Remote Working sind eine Herausforderung. Sie erhöhen das Risiko und erfordern ein Überdenken der Sicherheitsarchitektur und Technologien. Unternehmensführung und Verantwortliche für den Netzbetrieb haben ein höheres Risiko. Sie greifen auf geschäftskritische Systeme zu, ohne ein vergleichbares Maß an Sicherheitsvorkehrungen und Zugriffsbeschränkungen, denen andere Mitarbeitern unterliegen.

Abhilfe schaffen – Bei mittleren und kleinen Unternehmen wird die Akzeptanz von Endpoint und mobile Endpoint Management sowie Protection und Response-Lösungen (EPP) wachsen. Viele Unternehmen werden bei der Umsetzung auf einen Managed Security Service Provider zurückgreifen. Unternehmen, die aufgrund der Art der Daten, die sie verarbeiten, oder der Dienste, die sie anbieten, einem höheren Risiko ausgesetzt sind, werden wahrscheinlich verstärkt Managed Detection and Response (MDR)-Services einsetzen, um das Risiko durch raffinierte Bedrohungen weiter zu reduzieren.



Der schnelle Umstieg auf **Cloud-Dienste** zum Hosten von Systemen und Daten erhöht das Risiko von Datenschutzverletzungen und Service-Unterbrechungen in schlecht verwalteten Cloud-Umgebungen. Die Covid-19-Krise hat Initiativen zur digitalen Transformation und Cloud-Einführung beschleunigt. 2021 nimmt das Tempo weiter zu. Aber den meisten kleinen und mittleren Unternehmen fehlen immer noch die Sicherheitskontrollen, -prozesse und -fähigkeiten, um Transparenz über Cloud-Systeme hinweg zu gewährleisten und den eigenen Cloud-Footprint adäquat zu sichern.

Abhilfe schaffen – KMU werden ihre Sicherheitsprogramme an den Schutz von Cloud-Assets anpassen und ihre dahingehenden Anstrengungen intensivieren. Dabei richtet sich der Fokus auf Authentifizierung und Zugriffskontrolle, Cloud-natives Konfigurationsmanagement und Schwachstellenmanagement. Die wachsende Zahl von Sicherheitskontrollen und Tools auch in der typischen Umgebung mittlerer und kleiner Unternehmen gepaart mit der Herausforderung, Protection- sowie Detection-and-Response-Prozesse manuell zu orchestrieren, erfordern Veränderungen. KMU sind gezwungen, XDR-Analysetechnologien besser anzuwenden, um Sicherheitsvorfälle und -vorfälle insgesamt einfacher und effizienter zu orchestrieren und zu verwalten.

Anbieter von Managed und Professional Services werden aufgrund der Art der von ihnen verarbeiteten Daten, der von ihnen bereitgestellten Dienste oder der Systeme, auf die sie Zugriff haben, zunehmend gezielt angegriffen.

Abhilfe schaffen – Dazu ist die schnelle Einführung von EPP-Lösungen in den Netzwerken von Managed Services Providern von KMUs notwendig, wobei viele Unternehmen diese Funktion über spezialisierte Sicherheitsdienstleister in Anspruch nehmen. Anbieter von Managed Services oder Professional Services, die aufgrund der Art der von ihnen verarbeiteten Daten, der von ihnen erbrachten Dienste oder der Systeme, auf die sie Zugriff haben, einem höheren Risiko ausgesetzt sind, werden vermutlich verstärkt Managed Detection and Response (MDR)-Services einsetzen. Die senken das Risiko von ausgefeilten Bedrohungen, die sich potenziell von den eigenen Netzwerken in die Umgebungen ihrer Kunden ausbreiten oder Kundendaten in Mitleidenschaft ziehen.

MEHRSTUFIGE RANSOMWARE-ANGRIFFE NEHMEN 2021 AN REGELMÄSSIGKEIT ZU

Von Israel Barak

2020 beobachtete Cybereason weiterhin durchweg weniger Ransomware-Stämme in allen Netzwerken. Die allerdings erzielten deutlich höhere Gewinne. Hacker erreichen das vor allem durch ein gezieltes, mehrstufiges Vorgehen, um von jedem einzelnen Opfer mehr Lösegeld zu kassieren. 2021 rechnen wir mit einem Anstieg bei mehrstufiger Ransomware, eingebettet in Hacking-Operationen.

Krankenhäuser, Banken und kritische Infrastrukturen sind stärker gefährdet, aber betroffen sind viele Branchen. Erst nachdem Hacker eine Ransomware auf jedem Computer in einem Netzwerk platziert haben und weitere Angriffsstufen abgeschlossen sind, (wie z. B. Datendiebstahl, der Diebstahl von Benutzerpasswörtern und die Ausbreitung im Netzwerk), wird die Ransomware auf allen kompromittierten Endpunkten aktiviert.

Die gute Nachricht: Wer über einen schnellen Detection- und Response-Prozess verfügt, erkennt den Angriff in seinen frühen Stadien und kann effektiv reagieren, bevor die Ransomware in der Umgebung Schaden anrichtet.

Damit das gelingt, muss ein Unternehmen in erster Linie die Zeit minimieren, die es braucht, um auf Bedrohungen zu reagieren. Das erreicht man am besten durch Threat Hunting Services, die rund um die Uhr arbeiten.

Unter diesen veränderten Bedingungen reicht es nicht mehr aus, Resilienz und Sicherheit erst nachträglich in Betracht zu ziehen. Netzwerke der nächsten Generation sollten schon mit dieser Prämisse aufgebaut werden. Bei der Konzeption und im laufenden Betrieb sollte man auch berücksichtigen, welche Sicherheitsbedrohungen in den kommenden Monaten und Jahren vermutlich an der Tagesordnung sein werden.

Darüber hinaus sollten Unternehmen mit Experten zusammenarbeiten, die über ein umfangreiches Wissen zu Cyber-Bedrohungen verfügen. Öffentlicher und privater Sektor sollten eng kooperieren, wenn es darum geht, die Netzwerke von Banken, Krankenhäusern, Energieversorgern, der Luftfahrtindustrie und anderer kritischer Infrastrukturen wirksam zu schützen.

Und schließlich: Testen, testen, testen. Übungen, bei denen ein Red und ein Blue Team verschiedene Szenarien durchspielen und in Echtzeit darauf reagieren, geben wertvolle Hinweise für den Ernstfall, und sie unterstützen Führungskräfte dabei, den Stellenwert von Cybersicherheit wirklich zu verstehen.

XDR: EINE ZUKUNFT MIT EXTENDED DETECTION AND RESPONSE

Von Yonatan Striem-Amit, Chief Technology Officer und Mitgründer

Wir sind in einer „neuen Welt“, in der aktuellen Umfragen zufolge 2021 **fast die Hälfte der Arbeitgeber beabsichtigen, Mitarbeitern die Möglichkeit zu geben, dauerhaft von zu Hause aus zu arbeiten.** Mitarbeiter brauchen dann überall und jederzeit Zugriff auf das Unternehmensnetz, während gleichzeitig die Zahl und Komplexität von Cyberangriffen zunimmt.

Setzt Ihr Unternehmen Technologien ein, um korrelierte Angriffe auf sämtliche Benutzer, Geräte und Endpunkte in Ihrem Netzwerk zu stoppen? Wenn Sie mit Nein antworten, dann wird 2021 vermutlich ein hartes Jahr werden. XDR sollte Unternehmen in die Lage versetzen, ausgeklügelte Angriffe leichter zu erkennen, zu korrelieren und zu beenden, wo immer sie im Netzwerk auftreten. Durch die Kombination von Endpunkttelemetrie und Verhaltensanalyse für XDR haben Sicherheitsteams die Möglichkeit, Benutzer und Assets weltweit zu schützen.

Die Suche nach der richtigen XDR-Lösung muss nicht zwangsläufig mühsam sein, wenn man weiß, wie sie aussehen soll. Sicherheit beginnt damit, zu verstehen, was es zu schützen gilt. Eine XDR-Lösung sollte es Analysten aller Qualifikationsstufen erlauben, sich schnell in die Details eines Angriffs zu vertiefen, ohne erst komplizierte Abfragen zu erstellen. XDR erweitert dann die herkömmlichen Detection- und Response-Optionen vom Endpunkt bis hin zu kritischen SaaS-Diensten, E-Mail- und Cloud-Infrastrukturen.

XDR-Lösungen sollten Transparenz schaffen und Korrelationen zwischen den Indicators of Compromise (IOCs) und den wichtigsten Indicators of Behavior (IOBs), also den subtileren Anzeichen für ein kompromittiertes Netzwerk, herstellen und zudem verdächtige Benutzerzugriffe und Insider-Bedrohungen identifizieren.

Analysten sollten den kompletten Angriffsverlauf sofort verstehen und Abhilfe schaffen können. Sei es durch das Beenden eines Prozesses, eine Quarantäne oder die Remote Shell eines Systems, die entweder automatisiert oder remote mit einem einfachen Klick durchgeführt erfolgen kann. Im Idealfall verfügt eine XDR-Lösung über Funktionen, mit denen sich Bedrohungen automatisch beheben lassen und zusätzlich über ein kontinuierliches Threat Hunting.

XDR ist ein vielversprechender Ansatz, der den Vorteil des Angreifers umkehren und den Verteidigern wieder die Oberhand verschaffen kann. Dazu dehnt man die Detection und Response auf das breitere IT-Ökosystem aus, das moderne Unternehmensumgebungen ausmacht. Diese Vereinheitlichung erlaubt es, Malops im gesamten IT-Stack, wie z.B. Endpunkt-, Netzwerk- und Cloud-Bereitstellungen, aufzudecken.



DIE TRENDS AUF SEITEN DER VERTEIDIGER

Sam Curry, Chief Security Officer, Cybereason

Ein Jahr mehr und noch mehr Gejammer über noch mehr Datenschutzverletzungen. Ein Ende ist nicht in Sicht, obwohl wir mehr Absolventen in der Branche haben als je zuvor.

Wir können allerdings mehr tun, um Talente aus anderen Quellen zu rekrutieren. Der Trend zur Diversität hat gerade erst begonnen: Wir brauchen mehr Frauen, mehr Transgender, mehr Neurodiverse, mehr von allen.

Wir wollen die talentiertesten Mitarbeiter*innen, und wir müssen gewährleisten, dass, egal wo sie sind, egal welchen Hintergrund sie haben, eine Chance bekommen, bei uns mitzuarbeiten.

Wir können mehr tun, um den Stand der Technik voranzutreiben, Lehrpläne zu verbessern und andere aktiv zu ermutigen. Wir können und sollten hier nicht moralisch werden, aber darin liegt auch ein Wettbewerbsvorteil. Der Gegner ist divers, warum sollten wir das nicht auch sein? In der Diversität liegen Flexibilität, Optionen und Perspektiven.

Der Schlüssel zum Erfolg: im Cyberspace bekommt jeder eine Chance, wenn er es denn will – oder vielleicht will. In gewisser Weise müssen wir agiler werden. Dafür plädieren wir seit Jahren, gerade beim Thema Sicherheit. Jetzt *müssen* wir agiler darin werden, wie wir uns anpassen und weiterentwickeln.

Warum keine Retrospektive wie es gelaufen ist? Warum kein Sprint mit dem Ziel Diversität? Wenn wir unsere technischen Altlasten und Schulden in Sachen Sicherheit abbauen, warum sollten wir beim Mangel an geeigneten Fachkräften nicht genauso verfahren? Das sollten wir 2021 angehen!



Wichtige Erkenntnisse

Wir haben IoT aus den Unternehmen verbannt. Wer hätte gedacht, dass jetzt die Unternehmen zum IoT kommen! Der neue Adressraum eines Unternehmens sind Consumer-IPs, und die bösen Jungs wissen das. 2021 werden alte Exploits zurückkehren, veraltete Drucker und Router angreifen, und die DLP-Techniken umfunktionieren, um die Welt rund um kompromittierte Endpunkte und Bots herum zu erkunden. Das Schlimmste ist allerdings, dass die Allgegenwart des IoT bei einer schlecht gesicherten Haus-Automatisierung beginnt.

Die dunkle Seite war nicht untätig. Sie kann sich die Standard-Voice-to-Text-Funktion zunutze machen, um IP-Stacks in Privathaushalten zu kompromittieren und Informationen zu sammeln und ausgerüstet mit den besten Kameras und Mikrofonen, Speichern und Zugangsmöglichkeiten das Opfer auszuspionieren. Es ist an der Zeit, dass jemand ein Unternehmen gründet, das Support, Pflege, Sicherheit und vielleicht sogar Datenschutz auf IT-Level in die Haushalte bringt.

Wenn Unternehmen Zehntausende für Mitarbeiter zahlen, die in einem Büro sitzen, werden sie dann vielleicht eines Tages die Häuser der Mitarbeiter durch Outsourcing-Verträge zu einem Bruchteil der Kosten subventionieren und schützen, damit wir alle sicher und produktiv arbeiten können?

2021 wird es um "Arbeit von überall aus" gehen, ein ziemlich bewegliches Ziel für Sicherheitsexperten und Datenschutzfachleute. Wir müssen begreifen, dass sich auch der Gegner in eine neue Normalität bewegt. Vielleicht hat er derzeit noch keine Möglichkeit gefunden, alle Schwächen oder auch nur eine bestimmte Schwäche auszunutzen. Auch Cyberkriminelle konzentrieren sich erst Mal auf die naheliegenden Ziele. Was aber nicht heißt, dass sie nicht gleichzeitig in Forschung und Entwicklung investieren, um neuartige Angriffe speziell für die häusliche Umgebung zu konzipieren.

Bedrohungsakteure kaufen vielleicht Tools von anderen Cyberkriminellen, durchforsten bestehende Botnetze, um herauszufinden, welche IP-Adresse auf den bereits kompromittierten Geräten vorhanden ist, oder sie greifen Hausautomation, Drucker und Router an, nachdem sie IP-Adressen und digitale Standorte der Ziele trianguliert haben. Im kommenden Jahr wird es für die bösen Jungs das A und O sein, in neue Dimensionen der technischen Diversität vorzustoßen und innovative Angriffsvektoren zu entwickeln.

Es gab einmal eine Zeit, da ließen Hacker sich in übersichtliche Verhaltenskategorien einteilen, je nach Motivation oder Ziel. Zumindest wirkte es so. Im Laufe der Zeit waren die Kategorien dann nicht mehr ganz so zutreffend: Nationalstaaten wie Nordkorea hacken aus Profitgründen, um mit Wirtschaftssanktionen fertig zu werden, Cyberkriminelle vermieten ihre Dienste an alle möglichen Abnehmer und inzwischen bedienen sich auch Nationalstaaten bei Tools wie Ransomware. Um die Sache noch ein bisschen komplizierter zu machen, veröffentlichen Nationalstaaten wie etwa der Iran Tools, um Backdoors in der Welt der Cyberkriminalität zu platzieren und für ein ordentliches Hintergrundrauschen zu sorgen, Beamte offensiver Behörden von China bis Russland arbeiten schwarz oder gehen in Rente, ohne die Möglichkeit einer Operation unter falscher Flagge auch nur in Betracht zu ziehen.

Ein klarer *Modus Operandi* ist immer noch möglich. Das Nettoergebnis unserer Betrachtung ist allerdings: Kategorisierungsschemata im Allgemeinen und Attribution im Speziellen sind aktuell wenig hilfreich. Dieser Trend wird sich fortsetzen. Es ist ganz entscheidend sich auf alle Arten von potenziellen Angreifern vorzubereiten und blinde Flecken so weit als möglich zu vermeiden. Denn dadurch entsteht ein falsches Gefühl der Sicherheit darüber, wer der Feind ist.