Cyber Insights von Vodafone Business

AUSGABE 1: ORGANISIERTE INTERNETKRIMINALITÄT. Worum handelt es sich dabei eigentlich genau?

Finde mehr heraus

Together we can
vodafone
business

Inhalt

“Unsere Vision bei Vodafone Business ist es, Unternehmen, Mitarbeitern und Kunden Sicherheit zu bieten, wenn sie sich in der neuen digitalen Umgebung bewegen.

Wir unterstützen Ihr Unternehmen dabei, resilienter zu werden – egal, welche Stolpersteine Ihnen vor die Füße geworfen werden. Im Rahmen dieses Bestrebens haben wir unser vierteljährlich erscheinendes E-Book „Cyber Insights“ herausgebracht. Es soll Sie dabei unterstützen, mit der sich ständig verändernden Welt der Cyberrisiken Schritt zu halten. Es ist vollgepackt mit den neuesten Entwicklungen und nützlichen Erkenntnissen, um Ihr Unternehmen mit Sicherheit und Zuversicht vorwärtszubringen.

Internetkriminalität nimmt offensichtlich unaufhaltsam zu. Böswillige oder fahrlässige Insider, organisierte Kriminalität, Nationalstaaten und Hacktivisten stellen allesamt eine echte Bedrohung dar. Unternehmen stehen daher vor der sehr schweren Aufgabe, sich dagegen zu schützen. Dennoch heißt das nicht, dass der Kampf gegen die Internetkriminalität entmutigend, kompliziert oder kostspielig sein muss.

In dieser ersten Ausgabe werfen wir nun einen genaueren Blick auf einige der derzeit größten Bedrohungen der organisierten, internationalen Internetkriminalität – und die entsprechenden einfachen Maßnahmen, die Sie ergreifen können, um Ihr Unternehmen besser davor zu schützen.”

Andrzej Kawalec
Leiter des Bereichs Cybersicherheit bei Vodafone Business

Einleitung

Bei Cyberangriffen kommen nun verschiedene Taktiken und Gruppen zum Einsatz

Stellen Sie sich einen Cyberkriminellen vor. Wenn dabei eine Person in einem dunklen Raum, über einen Computer gebeugt, vor Ihrem inneren Auge erscheint, hätten Sie – vor fünf oder zehn Jahren – wahrscheinlich recht gehabt. Aber wie sieht es heute aus?

Stellen Sie sich ein paar Hundert Leute mehr vor, organisierte Teams und kriminelle Netzwerke, die sich über Ländergrenzen hinweg erstrecken. Die gefährlichsten Cyberkriminellen agieren wie internationale Unternehmen. Sie bilden Koalitionen und passen sich laufend an neue globale Trends an.

Im letzten Jahr haben Cyberkriminelle Covid-19, das Arbeiten im Homeoffice und soziale Anliegen wie „Black Lives Matter" ausgenutzt, nur um ein paar Beispiele zu nennen. In jüngster Zeit hat es auch eine Verschiebung dahingehend gegeben, dass organisierte Gruppen zunehmend Personen über Software und Systeme ins Visier nehmen. Diese Struktur, Zusammenarbeit und Anpassungsfähigkeit lässt die Anzahl der Angriffe stetig steigen. Cybersecurity Ventures geht davon aus, dass die weltweite Cyberkriminalität Unternehmen bis 2025 jährlich 10,5 Billionen US-Dollar kosten wird.[1]

Eines ist sicher. Alle Cyberkriminellen, ob organisiert oder nicht, entwickeln ihre Techniken laufend weiter. Die organisierten Cyberkriminellen können sich jedoch viel schneller weiterentwickeln und anpassen, da sie wahrscheinlich über die nötigen finanziellen Mittel verfügen. Einen Angriff bestimmten Gruppen, Ländern oder Motiven zuzuschreiben ist schon immer schwierig gewesen – und es wird immer schwieriger.

Oft werden mehrere Methoden in einem einzigen Angriff kombiniert, darunter:

Phishing nach Daten: Dabei senden Ihnen Betrüger eine gefälschte E-Mail und verleiten Sie zur Preisgabe Ihrer Daten.

Übernahme der Kontrolle Ihrer Computer: Dabei hacken Betrüger Ihre Geräte und übernehmen die Kontrolle darüber.

Installation von Ransomware: Dabei sperren Betrüger Ihre Dateien und erpressen von Ihnen Geld, um sie wieder freizugeben.

Hacking Ihrer Lieferkette: Dabei haben es Betrüger auf weniger sichere Elemente Ihrer Lieferkette abgesehen, um Ihrem Unternehmen Schaden zuzufügen.

Ausnutzen von Sicherheitslücken: Dabei suchen Betrüger nach Sicherheitslücken in Ihrer eigenen Software und Ihren Systemen sowie in denen von Drittanbietern und nutzen diese aus.

Verkauf oder Kauf von Malware: Dabei erwerben Betrüger Ransomware von oder bei einer anderen Bande, bekannt als Ransomware-as-a-Service (RaaS).

Mit Distributed Denial of Service (DDoS, engl. für „Verteilte Verweigerung des Dienstes"): Dabei versuchen Betrüger, Sie zur Zahlung von Lösegeld zu zwingen, indem sie DDoS als zusätzliches Druckmittel nutzen, das Ihre digitalen Dienste überlastet und diese dadurch für andere nicht mehr verfügbar sind.

Organisierte Cyberkriminelle wechseln mit der Zeit ihre Zugehörigkeiten, tauschen Hacker untereinander aus und ändern ihre Namen. Es ist auch nicht unüblich, dass, wenn eine Gruppe ein „erfolgreiches" Feature einsetzt, andere Gruppen nachziehen und diese Art von Angriff nachahmen. So entstehen Cyberkriminalitätstrends.

Aber es ist noch nicht aller Tage Abend! Wenn Sie in einem Erdbebengebiet leben, müssen Sie Ihr Haus auf eine bestimmte Art und Weise bauen. Im Moment befinden sich alle Unternehmen an einer Bruchlinie im Cyberspace. Um Cyberkriminalität zu bekämpfen, muss jedes Unternehmen und jeder Mitarbeiter genauso organisiert, proaktiv und unerbittlich wie die Kriminellen selbst sein. Die meisten Angriffe können vereitelt werden, wenn Sie Ihre Geräte, Software und Mitarbeiter stets auf dem neuesten Stand halten. Zudem können Sie Kriminellen den Garaus machen, indem Sie Betrügereien oder verdächtige Aktivitäten aufdecken.

Lassen Sie uns einen genaueren Blick auf drei der häufigsten Angriffsmethoden werfen, die derzeit in der organisierten Internetkriminalität zum Einsatz kommen – und auf einige der Maßnahmen, die Sie ergreifen können, um Ihr Unternehmen zu schützen.

Bedrohungsschwerpunkt 1:

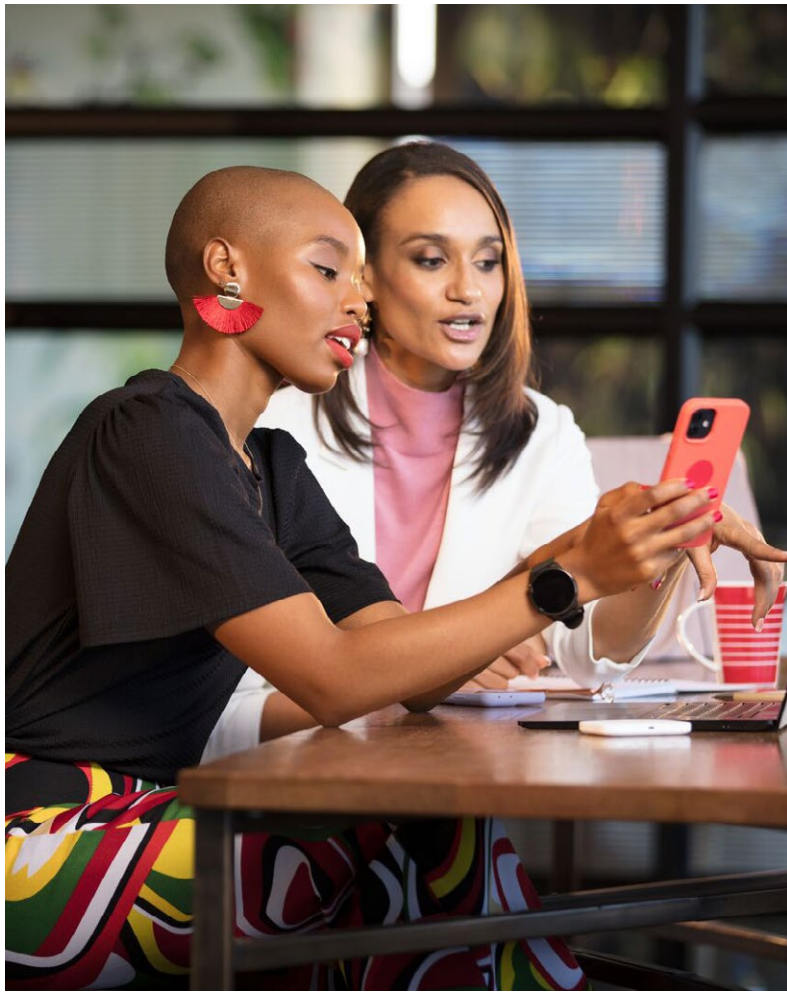
Ransomware und das Aufkommen von RaaS

Ein zunehmender Trend unter Cyberkriminellen sind Ransomware-Angriffe. Allein im Jahr 2020 gab es eine Zunahme der Ransomware-Angriffe um 150 % – und für das Jahr 2021 wird ein noch höherer Anstieg erwartet.[2] Der Grund dafür liegt auf der Hand: Im März 2021 erpresste die Ransomware-Bande REvil 50 Millionen US-Dollar von einem Computerhersteller – das höchste jemals gezahlte Lösegeld.[3] Tatsächlich stieg die Höhe des Lösegelds, das von den Opfern dieser Angriffe gezahlt wurde, im Jahr 2020 um mehr als 300 %.[4]

Diese Angriffe zielen darauf ab, Ihre Back-up-Dateien zu löschen, Kopien all Ihrer Daten zu erstellen und sie zu verschlüsseln. Somit kann niemand mehr auf diese Daten zugreifen. Alternativ werden Sie von den Betrügern erpresst und damit bedroht, dass sie Ihre Daten öffentlich machen oder weiterverkaufen, wenn Sie nicht zahlen. Die Akteure hinterlassen Ihnen eine Nachricht mit einer Lösegeldforderung, in der sie Ihnen mitteilen, wie Sie bezahlen sollen, um wieder auf Ihre Daten zugreifen zu können. Große kriminelle Hackergruppen wie FIN11 haben sich mittlerweile auf Ransomware und Datendiebstahlerpressung spezialisiert, da diese Taktiken sehr lukrativ sind und auch in nahezu jeder Organisation eingesetzt werden können.[5]

REvil ist ein Beispiel für eine Ransomware-as-a-Service(RaaS)-Unternehmung. Bei diesem Modell nutzen Cyberkriminelle Ransomware-Tools, die bereits von anderen Banden entwickelt wurden, um Ransomware-Angriffe durchzuführen. In dem besagten Fall verdient REvil, wenn das Opferunternehmen zahlt, etwa 20–30 % des erpressten Geldes und teilt sich den Rest mit Partnergruppen.[6]

Aufgrund der Funktionsweise von RaaS, die es Kriminellen mit wenig oder gar keinem technischen Wissen ermöglicht, in das Ransomware-Geschäft einzusteigen, wird diese Betrugsmethode unter Cyberkriminellen immer beliebter. Eine aktuelle Studie ergab, dass fast zwei Drittel der Ransomware-Angriffe im Jahr 2020 von Cyberkriminellen ausgingen, deren Vorgehensweise auf dem RaaS-Modell beruht [7].



Bedrohungsschwerpunkt 1:

Ransomware und das Aufkommen von RaaS

Fallstudie: Colonial Pipeline

Im Mai 2021 wurde die bittere Realität eines erfolgreichen Cyberangriffs enthüllt. Das US-amerikanische Unternehmen Colonial Pipeline – einer der größten Pipeline-Betreiber in den Vereinigten Staaten – musste nach einem Ransomware-Angriff der Cyber-Gang DarkSide vorübergehend den Betrieb einstellen und seine IT-Systeme einfrieren.[8]

DarkSide trat erstmals im August 2020 in Erscheinung und ist eine RaaS-Plattform, über die ausgewählte Cyberkriminelle Unternehmen mit Ransomware infizieren können. Sie verfügen über Komplizen, die die eigentlichen Angriffe auf die Zielnetzwerke durchführen, indem sie deren Daten stehlen und dann einen Ransomware-Code zur Verschlüsselung der Dateien installieren.

Sobald die Ransomware erfolgreich installiert ist, geht DarkSide in Verhandlungen mit den Opfern zwecks Lösegeldzahlungen. Sobald das Lösegeld gezahlt wurde, erhalten die für die Datensicherheitsverletzung verantwortlichen Komplizen den vereinbarten Prozentsatz des Lösegelds.

Im Fall von Colonial Pipeline – die etwa 45 % des Treibstoffs der US-amerikanischen Ostküste liefern – stahlen DarkSide-Angreifer 100 GB an vertraulichen Dokumenten, für die sie mit der Veröffentlichung drohten, falls das Lösegeld nicht gezahlt wird. Das Unternehmen gab zu, dass es Lösegeld in Höhe von 4,4 Millionen US-Dollar gezahlt hat, um die Systeme der Pipeline schnell und sicher wieder in Betrieb nehmen zu können.

Neueste Untersuchungen deuten darauf hin, dass es tatsächlich ein manipuliertes VPN-Konto war, das DarkSide den Zugriff auf die Daten ermöglichte. Das Passwort für dieses Konto wurde auf einer Liste von gestohlenen Passwörtern im Darknet gefunden, was bedeutet, dass ein Mitarbeiter dasselbe Passwort möglicherweise für ein anderes Konto verwendet hat, das zuvor gehackt wurde. Es ist überflüssig zu erwähnen, wie wichtig es ist, für jedes Konto ein eigenes Passwort festzulegen und nach Möglichkeit eine Multi-Faktor-Authentifizierung zu nutzen.

Wo ein Wille ist, ist auch ein Weg

Während Phishing nach wie vor die beliebteste Methode zur Verbreitung von Ransomware ist, werden Angriffe über das Remote-Desktop-Protokoll (RDP), bei denen Cyberkriminelle Ihren Mauszeiger kontrollieren können, und die Ausnutzung von Software-Schwachstellen allmählich immer häufiger. [9]

Dies ist auf die weit verbreitete Umstellung auf die Arbeit im Homeoffice zurückzuführen, die eine Reihe von Bedrohungen rund um den Remote-Zugriff mit sich gebracht hat. Schlecht konfigurierte Fernzugriffsdienste, wie RDP und Virtual Private Networks (VPN), ermöglichen Angreifern einen einfachen Zugriff auf Ihr Netzwerk. Es überrascht daher nicht, dass zwischen dem ersten und vierten Quartal 2020 die Zahl der RDP-Angriffe um 768 % gestiegen ist.[10]

Bedrohungsschwerpunkt 1:

Ransomware und das Aufkommen von RaaS

Cyberkriminelle Organisationen nutzen auch nicht gepatchte oder veraltete Software aus, um in Netzwerke einzudringen und Ransomware zu verbreiten. Im April 2021 deckte das FBI eine Reihe von Angriffen auf, die drei nicht gepatchte, kritische Schwachstellen in bestimmten Fortinet-FortiOS-Geräten ausnutzten, um sich zwecks Datendiebstahl und Datenverschlüsselung Zugang zu den Netzwerken der Opfer zu verschaffen.[11] Im März 2021 nutzten mindestens 10 verschiedene Gruppen von Cyberkriminellen Schwachstellen in der Mailserver-Software von Microsoft, um in Zielnetzwerke auf der ganzen Welt einzudringen.[12]

Cyberkriminelle Organisationen sind nicht wählerisch, vor allem wenn es um ein lukratives Geschäft wie Ransomware geht, bei dem im Durchschnitt 170.000 US-Dollar Lösegeld herausspringen.[13] Die Angriffspunkte sind mannigfaltig – und bei einer so hohen Gewinnaussicht werden sich die Banden mit Sicherheit zu helfen wissen.

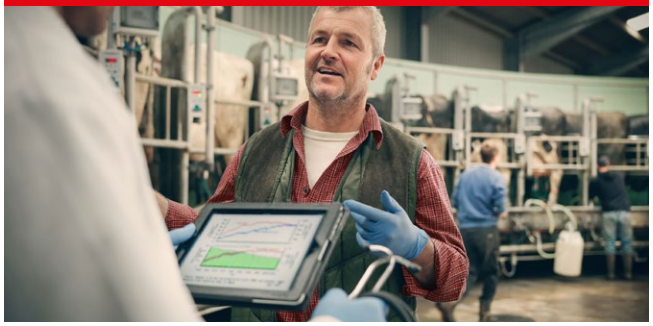
Tipp 1: Legen Sie Ihr Nähzeug beiseite: Was „Patchen“ wirklich bedeutet

Alle Smartphones, Tablets, Computer und Software, die Ihre Mitarbeiter nutzen, sollten fortlaufend regelmäßige Updates vom Hersteller erhalten. Im Rahmen dieser Updates werden nicht nur neue Funktionen hinzugefügt, sondern auch alle Sicherheitslücken geschlossen, die der Hersteller festgestellt hat.

Eines der wichtigsten Dinge, die Sie zur Erhöhung Ihrer Sicherheit tun können, ist, diese Updates direkt nach deren Bereitstellung zu installieren.[14] Und wenn ein Gerät, Betriebssystem, eine App oder Software nicht mehr unterstützt wird? Deinstallieren Sie diese/s und ersetzen Sie diese/s durch eine/s, das/die unterstützt wird. Es empfiehlt sich, nach Möglichkeit sämtliche Hard- und Software so einzustellen, dass sie automatisch aktualisiert wird. Das war´s schon! Das Ganze kommt ohne Nadelkissen und ohne komplizierten Code aus. Beim Patchen geht es darum, Ihre Systeme zu aktualisieren und zu verbessern – und zwar laufend.

Tipp 2: Wirklich nicht leicht zu knackende Passwörter? Wie Sie Ihr RDP nicht sichern

Es gibt mehrere Möglichkeiten, Ihr RDP gegen Brute-Force-Angriffe zu schützen. Sie werden in der Regel durch mangelnde Cyberhygiene verursacht – zum Beispiel durch schwache oder nicht vorhandene Passwörter an ihren Zugangspunkten. Sie sollten niemals ungeschützte Remote-Desktops im Internet veröffentlichen und stets sicherstellen, dass die Zugriffspunkte mit einer Multi-Faktor-Authentifizierung (MFA) geschützt sind. Das sorgt dafür, dass nur autorisierte Benutzer auf das RDP zugreifen können. Die Verwendung eines Remotedesktop-Gateways, das sich zwischen dem öffentlichen Internet und Ihren internen RDP-Geräten befindet, kann ebenfalls dazu beitragen, Angriffe abzuwehren.



Bedrohungsschwerpunkt 2:

Der Anstieg von Phishing, Vishing, Smishing und jetzt auch BEC

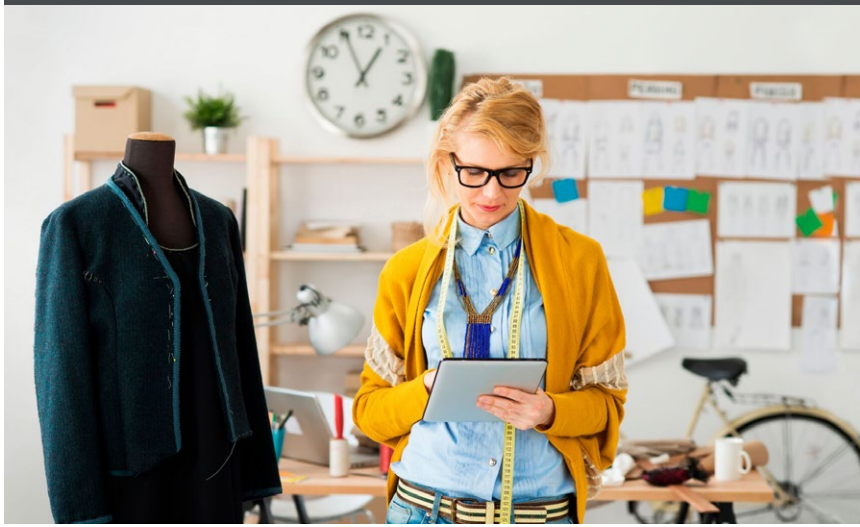
57 % der Unternehmen weltweit erlitten im Jahr 2020 einen erfolgreichen Phishing-Angriff.[15] Bei Phishing-Kampagnen senden Cyberkriminelle E-Mails an Ihre Mitarbeiter, um sie mit List dazu zu bringen, auf einer gefälschten Webseite persönliche Daten preiszugeben. Diese Daten nutzen sie dann, um in Ihr Netzwerk zu gelangen. Verglichen mit Ransomware ist diese Betrugsmasche leicht verdientes Geld. Es müssen kein Programm geschrieben und keine Viren verbreitet werden – eine vermeintlich seriöse E-Mail genügt. Eine neue Taktik besteht darin, diese E-Mails kurz nach einem Feiertag zu versenden, wenn die Posteingänge voll mit ungelesenen Mails sind, damit die betroffenen Personen sie aus Versehen öffnen.

Laut dem Transparenzbericht von Google und den von Atlas VPN analysierten Daten hat Google im Jahr 2020 über zwei Millionen Phishing-Webseiten registriert. Das sind durchschnittlich 46.000 neue Phishing-Websites pro Woche. Nach Angaben von Forbes stellt diese Zahl „einen Anstieg von 19,91 % im Vergleich zum gesamten Jahr 2019 dar, was darauf hindeutet, in welchem Maß die Coronapandemie die Möglichkeiten für Online-Betrug vervielfacht hat."[16]

Wie hat sich das in der Praxis ausgewirkt? Eine relativ kleine Studie von Cybersecurity Insiders unter 317 IT- und Cybersicherheitsexperten in den USA ergab, dass Unternehmen im Jahr 2020 durchschnittlich 1.185 Phishing-Angriffe pro Monat ausgesetzt waren. 53 % der Befragten gaben an, dass ihr Unternehmen eine Zunahme von E-Mail-Phishing-Angriffen während der Covid-19-Pandemie zu verzeichnen hatte. Zudem waren sich 36 % der Befragten nicht sicher, ob ihre Mitarbeiter einen E-Mail-Phishing-Angriff erkennen würden und vermeiden könnten.[17]

Hier sind einige der häufigsten Betreffzeilen, die Cyberkriminelle laut dem Phishing By Industry Report von KnowBe4 in E-Mail-Phishing-Versuchen im 4. Quartal 2020 verwendet haben.[18] Hinter den meisten Angriffen steht die Ausbeutung von Millionen von Menschen, die von zu Hause aus arbeiten:

- **Twitter:** Sicherheitswarnung: neue oder ungewöhnliche Twitter-Anmeldung
- **Amazon:** Handlung erforderlich | Ihre Amazon-Prime-Mitgliedschaft wurde abgelehnt
- **Zoom:** Fehler bei geplantem Meeting
- **Google Pay:** Zahlung gesendet
- **Microsoft 365:** Handlung erforderlich: Aktualisieren Sie die Adresse für Ihren Xbox Game Pass für das Konsolen-Abonnement
- **Workday:** Reminder: Wichtiges Sicherheitsupgrade erforderlich
- **DHL:** Ihr Paket ist auf dem Weg zu Ihnen. Verfolgen Sie es hier



Bedrohungsschwerpunkt 2:

Der Anstieg von Phishing, Vishing, Smishing und jetzt auch BEC

Ist Ihre Branche gefährdet? Oder macht Sie Ihre Größe zu leichter Beute?

KnowBe4 weist außerdem darauf hin, dass die am stärksten durch Phishing-Angriffe gefährdeten Branchen derzeit das Gesundheitswesen, die Fertigungsindustrie, das Bildungswesen, das Baugewerbe, das Unternehmensdienstleistungsgewerbe und die Technologiebranche sind. Expert Insights, die diese Ergebnisse veröffentlicht hat, fügt hinzu, dass kleine und mittelständische Firmen genauso gefährdet sind, Opfer eines Cyberangriffs zu werden, wie große Unternehmen. Da sie oft nicht über die nötige Infrastruktur oder notwendigen Ressourcen verfügen, um sich angemessen vor Angriffen zu schützen, werden sie von Kriminellen als leichte Beute ausgemacht.[19]

Vishing-Kriminelle können jetzt von der Nummer Ihrer Bank anrufen

Phishing bezieht sich auf E-Mails und Telefonanrufe, während bei Vishing – einer Kombination aus „Voice“ (Anruf) und „Phishing“ – ein Internet-Telefondienst (VoIP) zum Einsatz kommt. Die sogenannten Vishers geben sich als Unternehmen aus, entweder mittels einer aufgezeichneten Nachricht oder einer realen Person. Durch emotionale Manipulation werden Sie dazu gebracht, Ihre persönlichen Daten preiszugeben. Heute ist es möglich, von einer Nummer anrufen, die wie die tatsächliche Geschäftsnummer aussieht. Dies wird als Spoofing der Anrufer-ID bezeichnet. Solche Angriffe zielen derzeit auf Bankkunden ab.

Identitätsdiebe haben es auf Hauslieferungen abgesehen

Smishing ist eine Form des Phishings, bei der jedoch Textnachrichten (SMS) an Ihr Mobiltelefon gesendet werden. Darin enthaltende Links führen in der Regel auf eine gefälschte Webseite, die fast genauso aussieht wie die echte. Banden profitieren momentan von dem Umstand, dass so viele Menschen während der Coronapandemie Paketdienste in Anspruch nehmen. Diese Texte sehen also aus, als kämen sie von der Post oder einem Zustelldienst. Darin heißt es, sie hätten ein Paket für Sie. Um es zu erhalten, müssen Sie auf eine Webseite gehen, Ihre Daten eingeben und eine kleine Gebühr entrichten. 2,99 £ sind zwar nicht die Welt, aber es sind tatsächlich Ihre Daten, hinter denen die Betrüger her sind. Vor allem, wenn sie bereits andere persönliche Informationen über Sie haben, vielleicht durch einen Blick auf Ihre LinkedIn- oder Facebook-Seite. -

Fallstudie: FluBot und Android

Der Flubot-Betrug ist eine SMS-Betrugsmasche, bei der Android-Smartphones infiziert werden, und zwar über alle Mobilfunknetze hinweg. Eine SMS-Nachricht (Smishing), die angeblich von einer Reihe von Zustelldiensten wie FedEx und DHL stammt, informiert die Benutzer über den Status ihrer Paketzustellung, zusammen mit einem Link zur Nachverfolgung der Bestellung – hinter dem sich in Wirklichkeit ein Schadprogramm verbirgt.

Wird der Link angeklickt, werden schädliche Apps heruntergeladen (die das verschlüsselte FluBot-Modul hosten). Die Malware übernimmt die Kontrolle über das Gerät des Benutzers und sendet weitere infizierte Texte an dessen Kontakte. Sie trackt nicht nur die auf dem Gerät geöffneten Apps, sondern überlagert auch die Anmeldeseiten von Finanz-Apps mit schädlichen Programmen. Diese wurden entwickelt, um Anmeldedaten zu kapern und an Kontaktlisten, Nachrichten, Anrufe und Benachrichtigungen heranzukommen.

FluBot begann seine Machenschaften Ende 2020, wobei durch Kampagnen, bei der diese Malware zum Einsatz kam, bereits mehr als 60.000 Benutzer in Spanien infiziert wurden. Es soll mehr als 11 Millionen Telefonnummern von den Geräten gesammelt haben, was 25 % der Gesamtbevölkerung in Spanien entspricht. Laut einer neuen Analyse von Proofpoint haben die Bedrohungsakteure hinter FluBot (auch bekannt als Cabassous) inzwischen nicht nur Spanien, sondern auch Großbritannien, Deutschland, Ungarn, Italien und Polen ins Visier genommen.[20]

Proofpoint erklärt weiter: „FluBot wird sich wahrscheinlich weiterhin mit einer ziemlich hohen Geschwindigkeit ausbreiten und sich methodisch von Land zu Land durch gezielte Anstrengungen der Akteure bewegen. Solange es Benutzer gibt, die bereit sind, einer unerwarteten SMS-Nachricht zu vertrauen und den Anweisungen und Aufforderungen der Bedrohungsakteure Folge zu leisten, werden Kampagnen wie diese weiterhin von Erfolg gekrönt sein.“

Bedrohungsschwerpunkt 2:

Der Anstieg von Phishing, Vishing, Smishing und jetzt auch BEC

Ist diese E-Mail wirklich von Ihrem Chef?

Von Business Email Compromise (BEC) spricht man, wenn Sie eine Phishing-E-Mail erhalten, die so aussieht, als käme sie von Ihrem Unternehmen – möglicherweise sogar von Ihrem CEO. Die jüngsten BEC-Kampagnen zielen auf Covid-19-Impfungen und die Labore ab, die diese herstellen. Die Anzahl der Phishing- und BEC-Kampagnen wird in diesem Jahr weiter steigen, da die Cyberkriminellen ihre Taktiken stetig weiterentwickeln.

Die „Cosmic Lynx"-Bande ist vor Kurzem von der Verbreitung von Malware auf BEC-Angriffe umgestiegen – einem viel lukrativeren Geschäft. Seit Juli 2020 waren sie an über 200 BEC-Kampagnen beteiligt, bei der es die Betrüger auf Führungskräfte in 46 Ländern abgesehen hatten. Die Gruppe hebt sich von gewöhnlichen BEC-Betrugsmaschen ab, indem sie sich mittels äußerst professionell formulierter E-Mails und eines vorgetäuschten „Fusions- und Übernahme"-Szenarios größere Geldsummen erschleichen.[21]

Tipp 3: Verbreiten Sie das Bewusstsein für dieses Thema wie ein Lauffeuer – und machen Sie immer wieder auf aktuelle Betrugsmaschen aufmerksam

Alles, was ein motivierter Hacker braucht, um in Ihre Systeme einzudringen, ist, einen Mitarbeiter, der auf einen fragwürdigen Link klickt, ein leicht zu erratendes Passwort verwendet oder vergisst, sein Gerät oder seine Software zu aktualisieren. Stellen Sie sicher, dass Sie alle Mitarbeiter regelmäßig schulen, damit sie über die neuesten Bedrohungen – und wie sie sich davor schützen können – Bescheid wissen. Es braucht nur ein Schlupfloch ... und die Kriminellen sind drin.

Bringen Sie ihren Mitarbeitern den Unterschied zwischen einer seriösen und einer betrügerischen E-Mail (Scam) bei. Legen Sie ihnen nahe, bei allem skeptisch zu sein und alles Verdächtige zu überprüfen, bevor sie darauf klicken – indem sie das Ganze über einen anderen Kanal wie z. B. Google gegenprüfen. Vielleicht möchten Sie Ihre Mitarbeiter auch auf die Probe stellen: Versuchen Sie selbst oder mit Unterstützung Ihres Cybersicherheitspartners eine gefälschte E-Mail an sie zu senden. Verfassen Sie eine E-Mail, die sehr verdächtig erscheint, und eine, die schwerer als Betrugsmail zu erkennen ist. Wenn die Mitarbeiter darauf hereinfallen – und das werden sie – zeigen Sie ihnen, was sie eigentlich hätten tun sollen.

Cyberkriminelle ändern ihre Taktiken häufig. Daher ist es wichtig, auf neue Angriffsarten gefasst zu sein. Aktualisieren Sie Ihre Schulungsinhalte immer wieder mit den neuesten Betrugsmaschen, die die Runde machen, und beziehen Sie diese in Ihre Richtlinien mit ein, was zu tun ist, wenn Sie mit einer Verletzung Ihrer Datensicherheit konfrontiert sind. Ihr Technologieanbieter wird alle neuen Sicherheitslücken in den von Ihnen verwendeten Systemen bekannt geben – also überprüfen Sie auch diese.

Bedrohungsschwerpunkt 3:

Der dramatische Anstieg von APT- und Zero-Day-Angriffen

Im Dezember 2020 entdeckte SolarWinds (ein großes US-amerikanisches Technologieunternehmen) einen Angriff auf Kunden seines Netzwerkmanagementpakets: Orion. Die Orion-Software wird von einigen der größten Unternehmen der Welt genutzt, darunter der Mehrheit der umsatzstärksten US-amerikanischen Unternehmen aus der Liste „Fortune 500“ und zahlreicher Bundesministerien der US-Regierung (obwohl nach neuesten Untersuchungen das Pentagon ungeschoren davongekommen ist[22]). Brad Smith, Präsident von Microsoft, beschrieb das Eindringen in die Lieferkette von SolarWinds als „den größten und raffiniertesten Angriff, den die Welt je gesehen hat“.[23]

Experten gehen davon aus, dass eine in Russland ansässige Gruppe, die als Cozy Bear oder APT29 bekannt ist, hinter dem Angriff auf SolarWinds steckt. Der Cybercrime-Forscher Matthieu Faou schreibt den SolarWinds-Angriff zwar nicht Cozy Bear zu, vermutet aber, dass sich die Bande aus verschiedenen, kleineren Gruppen zusammensetzt. „Ich glaube, dass [Cozy Bear] aus mehreren Untergruppen besteht, die unterschiedliche Ziele und Werkzeuge haben.“ Faou fügt hinzu, dass die Gruppe „weit davon entfernt ist, monolithisch zu sein“.[24]

Hacker erreichen neue Stufen der Tarnung und Geduld

Die Untersuchungen des SolarWinds-Angriffs haben ergeben, dass es bereits im September 2019 Anzeichen für ein Eindringen in die Systeme gab. Die Cyberkriminellen versteckten sich, schwiegen und spionierten viele Monate lang. Dies wird als APT (Advanced Persistent Threat) bezeichnet. Oft werden Gruppen mit der Bezeichnung APT und einer Nummer versehen, da sie so von der US-Regierung klassifiziert werden.

Bedrohungsschwerpunkt 3:

Der dramatische Anstieg von APT- und Zero-Day-Angriffen

Die Gefahr von Zero-Day-Exploits

Bei der SolarWinds-Sicherheitsverletzung wurde eine Kombination von Methoden angewandt, wie z. B. das Ausprobieren gestohlener Daten auf mehreren Konten (Password-Spraying) und das Verbergen von Schadcode in anderen Dateien (Trojaner).[25] Die beunruhigendste Methode waren Zero-Day-Exploits oder „Zero-Day-Malware".

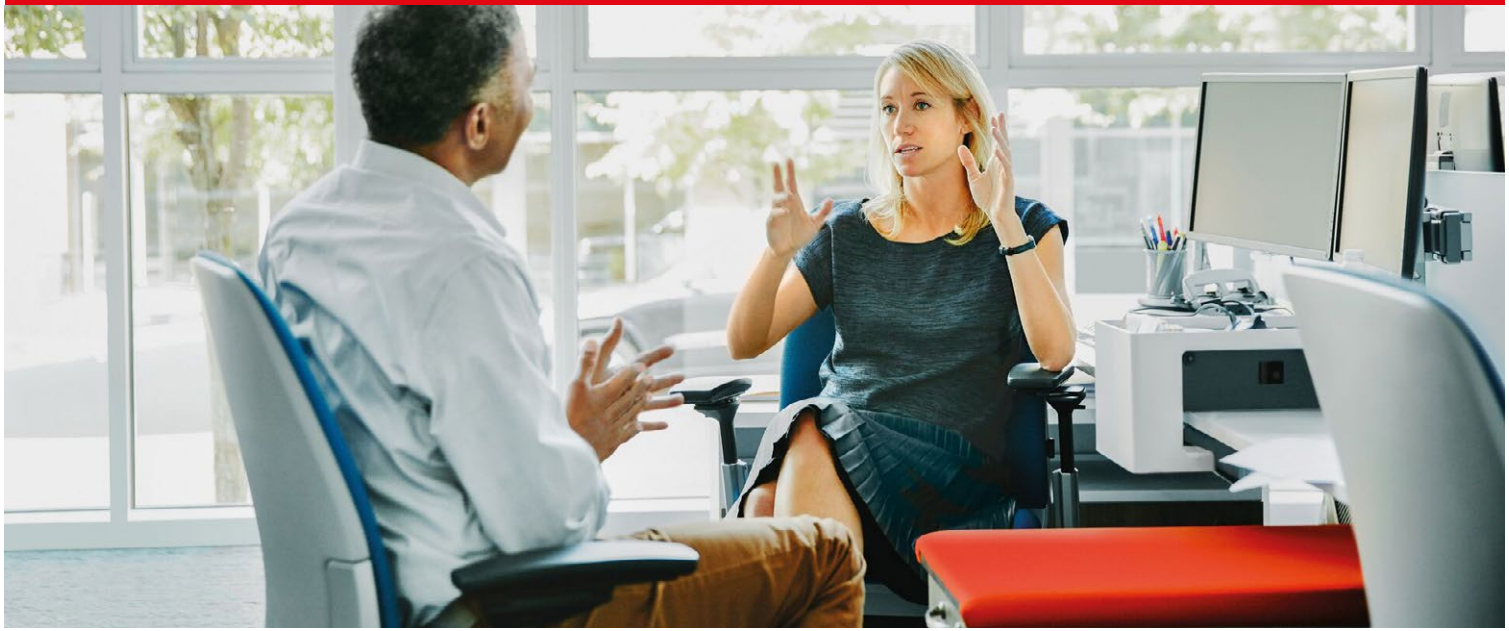
Dabei handelt es sich um Cyberangriffe, die stattfinden, bevor Ihr Technologielieferant einen Fix (Patch) für eine Sicherheitslücke oder „Schwachstelle" veröffentlicht hat. Wenn Sie von einer Schwachstelle in Ihrer Infrastruktur erfahren, können Sie diese normalerweise mit einem Patch beheben. Aber Zero-Day-Exploits sind besonders gefährlich. Sie haben einfach keine Zeit zum Handeln und auch keine Möglichkeit, die Schwachstelle zu beheben, bevor der Patch vom Hersteller veröffentlicht wird.

Im Jahr 2019 wurde 50 % der entdeckten Malware als Zero-Day-Bedrohungen klassifiziert[26] – und es liegen keine Anzeichen für eine rückläufige Entwicklung vor. Da organisierte Verbrechergruppen immer raffinierter werden, werden die Angriffe immer größer und dreister. Experten gehen davon aus, dass diese Zero-Day-Exploits im Jahr 2021 einmal pro Tag erfolgen werden, im Gegensatz zu einmal pro Woche im Jahr 2015.[27]

Tipp 4: Gehen Sie Ihre Sicherheitsprozesse immer wieder durch – und zwar regelmäßig

Es ist nicht immer möglich, Sicherheitsverletzungen zu verhindern, aber es ist wichtig, dass Sie diese sofort erkennen und darauf reagieren. Je schneller Sie sich von einem Angriff erholen, desto weniger starke Auswirkungen wird dieser auf Ihr Geschäft haben. Kein Grund zur Panik. Wenn ein Krimineller in Ihre Systeme eingedrungen ist, können Sie ihn noch stoppen. Wenn Sie denn merken, dass sich jemand Zugriff verschafft hat.

Stellen Sie also sicher, dass Sie einen Prozess implementiert haben, der kontinuierliches Patchen und regelmäßige, aktuelle Mitarbeiterschulungen umfasst. Und ganz wichtig – das können wir gar nicht oft genug betonen: Führen Sie die Schulungen regelmäßig durch. Nicht nur ab und zu.



Was kommt als nächstes?

Halten Sie Ausschau nach Ihrem nächsten E-Book „Cyber Insight“ – oder kontaktieren Sie uns

Bei Vodafone Business stellen wir Dienstleistungen und Wissen für Unternehmen jeder Größe bereit: für kleine, mittelständige oder große Unternehmen. Außerdem arbeiten wir mit marktführenden Sicherheitsdienstleistern wie SecurityScorecard und Recorded Future sowie mit Anbietern wie Accenture, Lookout, Trend Micro und IBM zusammen, um das bestmögliche Ergebnis für Ihr Unternehmen zu liefern.

Unabhängig von der Größe Ihres Unternehmens unterstützen wir bei Vodafone Business Sie mit vier einfachen Schritten – **Bewerten, Schützen, Erkennen, Reagieren** – um Ihre Systeme zu schützen und die Sicherheit Ihrer Mitarbeiter, Ihrer Standorte, Ihres Eigentums und Ihrer Daten zu gewährleisten.

Wir achten auf die Gefahren – und Sie halten einfach Ausschau nach der nächsten Ausgabe unseres E-Books „Cyber Insights“. Falls Sie Hilfe bei der Umsetzung einer dieser Tipps benötigen oder mehr darüber erfahren möchten, wie wir Ihr Unternehmen dabei unterstützen können, widerstandsfähiger zu werden, dann besuchen Sie bitte unsere **Website.**

(Oder – da Sie ja nie einem Link vertrauen sollten – geben Sie Vodafone Business Security in Ihre Suchmaschine ein).

Bewerten

Führen Sie eine vollständige Prüfung aller Geräte und Softwareprogramme durch, die in Ihrem Netzwerk verwendet werden. Denken Sie daran, dass jedes Gerät, das mit dem Internet verbunden ist, eine potenzielle Eintrittsmöglichkeit darstellt! Cyberkriminelle können das Passwort entweder mit roher Gewalt erzwingen, wobei sie jede Minute Tausende von Möglichkeiten erraten, oder sie umgehen das Problem einfach durch einen Fehler im Code. Achten Sie also auf eventuelle Sicherheitslücken. Sind die Geräte und Programme richtig konfiguriert? Sind die Passwörter sicher und willkürlich gewählt? Und was ist mit Ihren Lieferanten – haben diese Zugriff auf Ihre Daten? Wenn ja, sind deren Systeme sicher? Werden Ihre Passwörter irgendwo in einem beliebigen Dokument gespeichert?

Schützen

Halten Sie Ihre Geräte und Softwareprogramme durch die neuesten Versionen auf dem neuesten Stand. Entfernen oder deaktivieren Sie alles, was Sie nicht verwenden, und nutzen Sie eine Multi-Faktor-Authentifizierung, wo immer Sie können. Stellen Sie außerdem sicher, dass Sie eine Sicherungskopie aller Ihrer Daten haben. Das verhindert, dass Sie irgendwann einmal Lösegeld dafür zahlen müssen. Führen Sie regelmäßig ein Back-up durch, erstellen Sie mehrere Kopien und bewahren Sie mindestens eine Kopie extern und offline auf, um zu verhindern, dass Hacker diese löschen können.

Erkennen

Nutzen Sie Dienste wie Firewalls, IPS (Intrusion Prevention Systems) und IDS (Intrusion Detection Systems). Diese überwachen Ihr Netzwerk und warnen Sie vor möglichen Eindringlingen oder ungewöhnlichen Aktivitäten. Senden Sie alle Ihre Protokolle an einen zentralen Server und stellen Sie sicher, dass Sie die Protokolle überwachen und auf verdächtige Aktivitäten prüfen.

Reagieren

Wenn Ihre Systeme gehackt werden, müssen Sie in der Lage sein, schnell zu reagieren, um die Ausbreitung des Schadens zu stoppen. Sobald Sie von einer Sicherheitsverletzung Kenntnis erlangen, sollten Sie die Verbindung zum Netzwerk trennen und Ihren Vorfallsreaktionsplan zurate ziehen, um die entsprechenden Maßnahmen zu ergreifen. Schalten Sie die Server offline. Durchsuchen Sie diese dann und prüfen Sie, ob sich in den Daten ein verdächtiger Code verbirgt. Aktualisieren Sie alle Ihre Systeme, um sicherzustellen, dass sie über die neueste Version verfügen, und ändern Sie alle Passwörter. Es ist wichtig, mit einer spezialisierten Cybersicherheitsfirma zusammenzuarbeiten, der Sie vertrauen, damit diese Ihnen bei der Reaktion und Wiederherstellung im Falle einer Sicherheitsverletzung helfen kann. Vielleicht möchten Sie auch eine Cybersicherheits-Versicherung in Betracht ziehen.

Verweise

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybersecurity Ventures, 2020

2. Ransomware Attacks Are Spiking. Is Your Company Prepared?, Harvard Business Review, 2021

3. $50m ransomware demand on Acer is highest ever, ComputerWeekly, 2021

4. Ransomware Attacks Are Spiking. Is Your Company Prepared?, Harvard Business Review, 2021;

5. This major criminal hacking group just switched to ransomware attacks, ZDNet, 2020

6. REvil ransomware explained: A widespread extortion operation, CSO, 2020

7. Ransomware Uncovered 2020/2021, Group-IB, 2021

8. Colonial Pipeline attack: Everything you need to know, ZDNet, 2021

9. Top 3 Attack Vectors Ransomware Loves to Exploit, Digital Defense

10. RDP Attacks Persist Near Record Levels in 2021, Dark Reading, 2021

11. FBI: Unpatched Fortinet Flaws Remain Under Attack by APT Actors, 2021

12. At least 10 hacking groups using Microsoft software flaw: researchers, Reuters, 2021

13. The average ransomware demand is now $170K. Here's how we can fight back, World Economic Forum, 2021

14. Cyber security for your organisation starts here, National Cyber Security Centre UK

15. Phishing attack victimization among businesses worldwide 2020, Statista, 2020

16. Google Registers Record Two Million Phishing Websites In 2020, Forbes, 2020

17. 2020 Phishing Attack Landscape Report [Greathorn], Cybersecurity Insiders, 2020

18. 2020 Phishing By Industry Benchmarking Report, KnowBe4, 2020

19. 50 Phishing Stats You Should Know In 2021, Expert Insights, 2021

20. FluBot Android Malware Spreading Rapidly Through Europe, May Hit U.S. Soon, Proofpoint, 2021

21. First-Ever Russian BEC Gang, Cosmic Lynx, Uncovered, Threat Post, 2020

22. Pentagon believes it escaped unscathed from SolarWinds, Microsoft hacks, Federal News Network, 2021

23. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president, Reuters, 2021

24. How the Russian hacking group Cozy Bear, suspected in the SolarWinds breach, plays the long game, CyberScoop, 2020

25. FBI, CISA Uncover Tactics Employed by Russian Intelligence Hackers, The Hacker News, 2021

26. As malware and network attacks increase in 2019, zero day malware accounts for 50% of detections, HelpNetSecurity, 2019

27. Zero Day Report 2017, Cybersecurity Ventures, 2017

Together we can

vodafone business