Trends & Technologien

Die COVID-19-Pandemie hat Deutschland auch im Jahr 2021 im Griff und treibt die Zahl der in Heimarbeit Beschäftigten in die Höhe. Beste Voraussetzungen für Kriminelle, denen die große Zahl an Homeoffice-Arbeitsplätzen viele neue Angriffspunkte für Cyberattacken beschert. Großangelegte Einfallversuche durch Remote-Angriffe, Phishing und Social Engineering sind an der Tagesordnung. Und immer öfter richten Hacker massiven Schaden an.

Neue Angriffsvektoren

Wie Sie 2021 gehackt werden

Dieses Jahr werden kriminelle Hacker alles daransetzen, die Effizienz ihrer Angriffe weiter zu steigern. Im Fokus stehen vor allem Corona-bedingte Schwachstellen.

Die Corona-Pandemie hat das gesamte Unternehmensumfeld seit März letzten Jahres komplett aus den Angeln gehoben – insbesondere auch, was die Bedrohungslandschaft angeht. Das ist eigentlich kein Wunder angesichts der Tatsache, dass die Umstellung auf Remote Work in den meisten Fällen in wenigen Tagen abgewickelt werden musste, um den Geschäftsbetrieb am Laufen zu halten.

› COVID-19 hat nicht nur das Business grundlegend verändert, sondern auch die Angriffsflächen der Unternehmensnetzwerke. Das kommt in Sachen Security 2021 auf Sie zu. (Bild: issaro prakalung, Shutterstock.com)

Folglich sorgte COVID-19 auch für einen noch stärkeren Run auf – beziehungsweise in – die Cloud, als ohnehin erwartet worden war. Der plötzliche Umschwung auf Remote-Arbeit sorgt dafür, dass circa 90 Prozent der Datenflüsse nicht mehr über interne, sondern externe Systeme abgewickelt werden. Auch IoT Devices erfreuen sich steigender Beliebtheit. Die Mehrheit dieser Gerätschaften für Endverbraucher ist dabei weiterhin unzureichend abgesichert. Für Cyberkriminelle ein willkommener Anlass, sich Zugang zu sensiblen Systemen und Daten zu erschleichen.

Angesichts der veränderten Bedrohungslandschaft wäre zu erwarten, dass CISOs auch neue Security-Strategien und -Tools einsetzen. Leider ist jedoch vielerorts keine Neupriorisierung der Sicherheitsinitiativen in Sicht: Zwar nahm das Volumen der Angriffe insgesamt und ihre Intensität zu, die spezifischen Kompromittierungsmethoden der Cyberkriminellen haben sich bislang jedoch nicht maßgeblich verändert. Doch das dürfte sich nun ändern, wie die Kollegen unserer US-Schwesterpublikation **CSO Online** (*www.csoonline.com*) im Gespräch mit zahlreichen Security-Experten herausgefunden haben. Lesen Sie, wie Sie 2021 gehackt werden sollen.

Passend zum Thema:

› Die IT-Sicherheit braucht eine Neuorientierung (**Seite 54**)
› Home Office fordert die Cybersecurity (**Seite 60**)

Remote Hacks Reloaded

Über Remote Devices fließen in Homeoffice-Umgebungen heute deutlich mehr sensible Unternehmensdaten als vor der Corona-Pandemie. Auch deswegen erwartet Jim Boehm, Partner bei der Unternehmensberatung **McKinsey** (*www.mckinsey.de*), neue Angriffsmethoden, die sich auf diese Gerätschaften fokussieren. Als Beispiel führt der Sicherheitsexperte einen Kunden an, bei dem die VPN-Protokolle mehr auf Business Continuity als auf Security ausgerichtet waren: Wurde die Verbindung zum VPN unterbrochen, standen weiterhin Basis-Funktionalitäten zur Verfügung, wie Boehm ausführt: „Wenn der E-Mail-Client vor der Verbindungsunterbrechung mit dem VPN konnektiert war, wurden WebEx-Sessions und Datentransfers wieder aufgenommen. Das hat zu einem Exploit geführt, den Cyberkriminelle dazu nutzen könnten, Devices zu kompromittieren – noch bevor eine VPN-Verbindung zustande kommt."

Ein akzeptables Risiko, wenn nur zehn Prozent des Datenverkehrs über VPN läuft. Nachdem sich das Verhältnis jedoch umgedreht hat und 90 Prozent der Daten über getunnelte Verbindungen fließen, sollten CISOs an dieser Stelle über eine Neupriorisierung nachdenken. Schließlich werden Virtual Private Networks auch in den kommenden Jahren im Unternehmensumfeld Usus bleiben. „In einer Welt, die komplett

auf Zero Trust setzt (mehr zum Thema ab **Seite 106**), können Sie auf VPN verzichten. Das einzige Unternehmen, das heute bereits eine reine Zero-Trust-Architektur hat, ist Google", ergänzt Boehm.

Cloud-Konfigurations-Fails

Angriffe über die Cloud sind ein weiterer Pain Point, wie Chet Wisniekski, Chef-Researcher bei **Sophos** (*www.sophos.com*), weiß. Seiner Meinung nach befinden sich Cloud-Konfiguration und menschliche Natur auf einem Kollisionskurs – während Cyberkriminelle sich bereithalten, um genau das auszunutzen.

Um das an einem Beispiel zu verdeutlichen, erzählt der Security-Spezialist von einem Großkunden, der Cloud-Instanzen bei mehreren großen Anbietern eingekauft hatte: „In Sachen Passwort-Komplexität, Default-Einstellungen oder was das Aufsetzen neuer Instanzen angeht, gibt es je nach Anbieter große Unterschiede. In der Google Cloud müssen beispielsweise viele Dinge manuell konfiguriert werden, die bei Azure und AWS automatisch voreingestellt sind. Das Problem dabei: Je ausgeprägter das Wissen über die eine Umgebung, desto effizienter lässt sie sich nutzen – mit zunehmender Expertise für das eine Deployment steigt jedoch auch die Wahrscheinlichkeit, dass Konfigurationsfehler in anderen, weniger vertrauten Umgebungen auftreten."

Inkonsistenzen innerhalb derselben Plattform sowie Schatten-Accounts von denen weder CISO noch CIO etwas wissen, verstärken das Security-Problem noch, das durch fehlerhafte Cloud-Konfigurationen entstehen kann. Besonders relevant wird das im Regelfall, wenn mehrere Instanzen verschiedener Anbieter eingesetzt werden. Um an Zugangsdaten und andere Unternehmensinformationen zu kommen, setzen kriminelle Hacker alles daran, diese Art der Verwirrung auszunutzen – und sind dabei bestens über die Cloud-Angebote und -Fallstricke der einzelnen Anbieter (mehr dazu ab **Seite 110**) informiert, wie Wisniekski weiß.

Remote-Office-Gefahren

Viele Remote-Work- und Homeoffice-Setups im Enterprise-Umfeld sind viel zu komplex ausgestaltet, was möglicherweise zu Inkonsistenzen führt, die Angreifer für maliziöse Zwecke ausnutzen können.

„Die Diversität der Heimnetzwerk-Konfigurationen ist atemberaubend – man findet Setups, die man so nicht für möglich gehalten hätte", plaudert John Henning, Chef-Security-Engineer bei **SAS** (*www.sas.com*), aus dem Nähkästchen. „Der Versuch, bei einem Heimnetzwerk Fern-Support zu leisten, frisst enorme Ressourcen, bringt aber

im Regelfall keinen Ertrag", so der Experte weiter. „Ein gelungener Return-on-Investment ist meiner Meinung nach nur über die konsequente Schulung der User zu erzielen – im Idealfall anhand von Best Practices."

Dabei sieht Henning überraschenderweise vor allem die tech-affinen User in problematischem Licht. Diese würden einen Hang dazu aufweisen, mit ihren Heimnetzwerken – beziehungsweise deren Konfiguration – zu experimentieren: „Unkundige Benutzer werden das nicht tun. Obwohl Standardeinstellungen nicht ideal sind, bieten die meisten aktuellen Geräte auf dem Markt mit Default Settings bereits ein akzeptables Security-Niveau", so Henning.

Darüber hinaus bereiten dem Security-Spezialisten von Sophos auch Open Source Intelligence Tools: „Angreifer nutzen öffentlich zugängliche OSINT-Tools wie Shodan, um angreifbare Devices von Mitarbeitern aufzuspüren. Es ist ohne weiteres möglich, bei der Suche mit Shodan und Co. auch auf sensible Unternehmensdaten oder Einfallsmöglichkeiten in Firmennetzwerke zu stoßen."

Tunnel im Tunnel

Da sich 2021 am VPN-Datenaufkommen nicht viel ändern wird, ist zu erwarten, dass auch Cyberkriminelle zunehmend versuchen werden, VPN-Systeme als direkten Zugangspunkt zu Unternehmenssystemen zu nutzen.

VPN-Nutzer, beziehungsweise -Systeme im Netzwerk zu identifizieren, sei dabei relativ leicht, weiß Corey Nachreiner, CTO bei **WatchGuard Technologies** (*www.watchguard.com*): „Die meisten Trojaner oder Bot Clients erlauben den Angreifern, manuell oder automatisiert Befehle auszuführen. Das reicht bereits, um VPN-Software aufzuspüren – beispielsweise über den ipconfig-Befehl. Automatisierte Malware lässt sich gezielt auf VPN-Verbindungen ausrichten – entsprechende Systeme werden geflaggt und ein Alert an den Angreifer versendet. Von hier aus können Cyberkriminelle mit Hilfe von Wurm-Funktionalitäten und Techniken, mit deren Hilfe sie sich lateral durch Netzwerke bewegen, Angriffe auf VPN-Netzwerke starten."

Malware auf KI-Basis

Kriminelle Hacker, die künstliche Intelligenz und Machine Learning für ihre Angriffe instrumentalisieren, sind ein Szenario, das schon länger heraufbeschworen wird. 2021 könnte es „endlich" soweit sein, wie Ben Goodman, Senior Vice President von **ForgeRock** (*www.forgerock.com*), prophezeiht: „2021 werden wir nicht nur sehen, dass das Deployment von KI-Plattformen in Unternehmen deutlich anziehen wird, sondern auch

eine deutliche Zunahme bei Data-Poisoning-Attacken verzeichnen. Schon in den letzten Jahren haben Cyberkriminelle KI- und Machine-Learning-Software erfolgreich kompromittiert, indem sie die Systeme mit schädlichen Daten gefüttert haben."

Die „Vergiftung" von KI-Algorithmen mit Daten werde laut dem Experten in den kommenden Jahren weiter zunehmen. Weil auch im Security-Bereich die KI-Adoption weiter zunehme, sieht Goodman dunkle Wolken aufziehen: „Im kommenden Jahr könnte es nötig werden, eine eigene KI-Instanz zu schaffen, die ausschließlich dafür da ist, die von anderen KI-Systemen aggregierten Daten auf Integritäts- und Sicherheitsaspekte hin zu überprüfen."

Quantencomputer-Dystopie

Dass Cyberkriminelle schon im kommenden Jahr hochgezüchtete Quantencomputer nutzen, um Unternehmen zu kompromittieren, ist eher unwahrscheinlich. Angesichts der dauerhaften „Bemühungen" verschiedener Staaten (Russland, Nordkorea oder Iran, um nur einige zu nennen) liegt es aber dennoch im Bereich des Möglichen. Steve Zalewski etwa, Deputy CISO bei Levi Strauss & Co. (*www.levi.com*), blickt mit Sorge auf die Möglichkeiten, die Quantum Computing bietet, um die Verschlüsselung von Unternehmensdaten aus den Angeln zu heben.

„Das wäre ein Gamechanger," so der Security-Spezialist. „Quantencomputing ist derzeit eine Lösung, für die noch das passende Problem gesucht wird. Frühe Supercomputer etwa waren zwar gut für Simulationen geeignet, aber nicht für herkömmliche Rechenaufgaben. Das könnte kriminellen Hackern in Zukunft zum Vorteil gereichen."

Evan Schuman
und Florian Maier

Evan schreibt als freier Autor und Kolumnist unter anderem für CBS News, RetailWeek und eWeek sowie für unsere US-Schwesterpublikationen Computerworld, CSO Online und CIO.com.

Florian Maier beschäftigt sich mit vielen Themen rund um Technologie und Management. Daneben betätigt er sich auch in sozialen Netzen.