**MEDIENINFORMATION**

Zürich, 23. November 2020

**Automatisierung als Freund und Feind der IT-Sicherheit**

**Trends 2021: Automatisierung wird Flutwelle an Spear-Phishing auslösen und gleichzeitig Cloud Providern als Waffe gegen Angreifer dienen**

Nachdem sich das Jahr 2020 langsam dem Ende zuneigt, ist es für die IT-Sicherheitsexperten von WatchGuard Technologies an der Zeit, den Blick gezielt nach vorn zu richten. Auf Basis der aktuellen Faktenlage lassen sich stichhaltige Rückschlüsse ziehen, welche Trends das IT-Security-Umfeld in den kommenden Monaten prägen werden und worauf sich Unternehmen jeder Grösse sowie Branche einstellen sollten. Eine wichtige Rolle spielt in dem Zusammenhang die Automatisierung – sowohl auf Seiten der Angreifer als auch bei der Bedrohungs­abwehr. So ist beispielsweise zu erwarten, dass Automatisierungs­werkzeuge manuelle Herangehensweisen im Rahmen von Spear-Fishing-Attacken zunehmend ersetzen werden, um zum einen Social-Media-Kanäle und Unternehmenswebseiten im grossen Stil nach individuellen Informationen abzusuchen. Zum anderen lassen sich die gesammelten Daten dank der neuen Möglichkeiten ebenso schnell und automatisiert missbrauchen. Es ist in dem Zusammenhang sehr wahr­scheinlich, dass Cyberkriminelle weiterhin mit Ängsten rund um Pandemie und wirtschaftliche Verluste spielen.

Gleichzeitig werden moderne Automatismen aber auch im Kampf gegen die Bedrohung vermehrt ihre Wirkung entfalten und Anbietern von Cloud-Plattformen wie Amazon, Microsoft und Google dabei helfen, gegen cyberkriminelle Gruppen vorzugehen, die vertraute Dienste für böswillige Angriffe ausnutzen. In der Vergangenheit liess sich immer wieder beobachten, wie legitime Webseiten – beispielsweise von Microsoft365 oder Google Drive – imitiert wurden, um von ahnungslosen Opfern selbst eingegebene Daten zu stehlen. Hier werden Provider künftig auch beim Aufspüren solch gefälschter Anmeldeseiten auf Automatisierungswerkzeuge und Validierungs­technologien setzen – mit dem Ziel, der Gefahr entgegenzusteuern.

Darüber hinaus sehen die WatchGuard-Analysten weitere Trends, die auf der [WatchGuard-Webseite](https://www.watchguard.com/de/wgrd-resource-center/cyber-security-predictions-2021) im Detail vorgestellt werden. Einige der Prognosen im Überblick:

Homeoffice-Szenarien rücken VPN und RDP ins Visier der Hacker

Da immer mehr Unternehmen VPN- und Remote Desktop Protocol (RDP)-Lösungen einsetzen, um sichere Verbindungen für die von zu Hause aus agierenden Mitarbeitenden bereitzustellen, rechnet WatchGuard mit einer Verdoppelung darauf ausgerichteter Angriffe. Sobald es Hackern gelingt, VPN, RDP oder Fernverbindungsserver zu kompromittieren, ist der Sprung ins Unternehmensnetzwerk kaum aufzuhalten.

Ungepatchte Endgeräte werden zum Verhängnis

Aufgrund der Pandemie sind Mitarbeitende und ihre Endgeräte an vorderste Front gerückt. Dabei läuft auf zahlreichen Rechnern noch immer veraltete Software, die schwer zu patchen oder zu aktualisieren ist. Da im Januar 2021 beispielsweise auch der Support für Microsoft Windows 7 endet, rät WatchGuard Unternehmen hier zu besonderer Vorsicht. Laut den Experten wird mindestens eine grössere neue Windows 7-Schwachstelle in den kommenden Monaten für Schlagzeilen sorgen.

Multifaktor-Authentifizierung als Zünglein an der Waage

Angesichts der Milliarden Benutzernamen und Passwörter, die im Dark Web frei zugänglich sind, sowie vor dem Hintergrund des Siegeszugs automatisierter Authentifizierungsangriffe gehen online-basierte Dienste mit klassischer Einwahlmöglichkeit ein immer grösseres Risiko ein. Tatsächlich sieht WatchGuard alle Anwendungen, die nicht über das zusätzliche Schutzschild der Multifaktor-Authentifizierung verfügen, in Gefahr.

„2020 hat gezeigt, wie schnell sich Rahmenbedingungen ändern können. Dies hat dann natürlich auch Einfluss auf Prognosen“, so Corey Nachreiner, CTO bei WatchGuard Technologies. „Nichtsdestotrotz ist unser Threat Lab-Team – im Einklang mit anderen Analysten auf der ganzen Welt, die tief im Thema stecken – auf Basis weitreichender Analysemöglichkeiten in der Lage, fundierte Vermutungen anzustellen. Cyberkriminelle suchen immer nach den schwächsten Gliedern in der Abwehrkette. Durch die Zunahme der Heimarbeit ergibt sich eine neue, attraktive Angriffsfläche. Zudem ist davon auszugehen, dass neue Technologien rund um Automatisierung und KI nicht den ‚Guten‘ überlassen werden. Letztlich geht es allein darum, der Gegenseite den entscheidenden Schritt voraus zu sein.“

Weitere Informationen zu den von WatchGuard prognostizierten IT-Security-Trends für 2021 einschliesslich Videos stehen online zur Verfügung: <https://www.watchguard.com/de/wgrd-resource-center/cyber-security-predictions-2021>

Bildmaterial

|  |
| --- |
|   |
| Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies |

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „[Corey Nachreiner](https://press-n-relations.amid-pr.com/AMID-PR/searchresult/searchresult.xhtml?searchString=Corey+Nachreiner&searchId=1&searchType=detailed)"). Selbstverständlich schicke ich Ihnen die Datei oder eventuell gewünschte Schmuckbilder auch gerne per E-Mail zu. Kontakt: rh@press-n-relations.de

|  |  |
| --- | --- |
| Kontakt:WatchGuard Technologies GmbHPaul Moll – Field Marketing Manager Central EuropeWendenstr. 379, 20537 HamburgTel.: +49 152 31795040paul.moll@watchguard.comwww.watchguard.de | Presse- und Öffentlichkeitsarbeit:Press'n'Relations GmbH, c/o Medianovis AGRebecca HornSchaffhauserstr. 91, 8057 ZürichTel.: +49 731 962 87 15 rh@press-n-relations.dewww.press-n-relations.com |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich IT-Sicherheit. Das umfangreiche Produktportfolio reicht von hochentwickelten UTM (Unified Threat Management)- und Next-Generation-Firewall-Plattformen über Multifaktor-Authentifizierung bis hin zu Technologien für umfassenden WLAN-Schutz und Endpoint Protection sowie weiteren spezifischen Produkten und Services rund ums Thema IT-Security. Mehr als 80.000 Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung neben kleinen und mittelständischen Unternehmen nicht zuletzt auch grosse, dezentral aufgestellte Organisationen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Aktuelle Informationen, Aktionen und Updates finden Sie auch auf [Twitter](https://twitter.com/sichersein), [Facebook](https://de-de.facebook.com/WatchGuardSichersein/) oder [LinkedIn](https://de.linkedin.com/company/watchguardsichersein). Der WatchGuard-Blog „Secplicity“ berichtet darüber hinaus über die neuesten Bedrohungen und zeigt auf, wie man mit ihnen umgeht: [www.secplicity.org](http://www.secplicity.org/). Oder Sie abonnieren den „443 - Security Simplified“-Podcast bei [Secplicity.org](http://www.secplicity.org/) bzw. wo immer Sie Ihre Lieblings-Podcasts finden.