„Alles gut, weil bis jetzt ist nichts passiert“ ist die schlechteste Cybersicherheitsstrategie. Der Safer Internet Day erinnert Unternehmen und Anwender daran, wie es besser geht.

Das Internet sicher zu machen, ist eine Utopie, aber jeder kann sein eigenes Verhalten im Umgang mit dem Internet so gestalten, dass die Nutzung möglichst sicher ist. Aus diesem Grund ist der Safer Internet Day am 6. Februar eine gute Gelegenheit, das eigene Tun und Handeln sowie das des Unternehmens auf den Prüfstand zu stellen.

Ein wichtiger Aspekt für die sichere Internetnutzung ist gleichzeitig einer, den niemand so richtig gerne mag: Passwörter. Und dennoch ist das Passwort für jeden User und für alle Unternehmen eine der besten Schutzmöglichkeiten. Indem mit guten Passwörtern und mit einer Zwei-Faktor-Authentifizierung oder noch fortschrittlicheren Technologien der unautorisierte Zugang zu Computern, Netzwerken und Applikationen verhindert wird, sind Cyberkriminelle nicht in der Lage einzudringen, ihre Privilegien auszuweiten und schlussendlich Ransomware zu aktivieren oder wertvolle Daten zu stehlen.

„Obwohl kaum jemand das Anlegen, Verwalten und den Umgang mit Passwörtern mag, weiß jedes Unternehmen und jeder Internet-Nutzende, dass sie trotz aller Lästigkeit enorm wichtig sind. Allerdings sehen wir, wie selbst große Konzerne aufgrund einer schlechten Passwortverwaltung oder einem laxen Umgang kompromittiert werden. Die Verwendung guter Passwörter für jede Website gehört in Verbindung mit weiteren zusätzlichen Authentifizierungsmethoden nach wie vor zu den besten Maßnahmen, um kritische Zugänge und das Unternehmen zu schützen", merkt Michael Veit, Sicherheitsexperte bei Sophos, an.

Nicht nur gemutmaßt, sondern Fakt
Aussagen wie „es wird schon alles gut gehen“ oder „das sind ja keine wichtigen Accounts“ oder „ich habe gerade keine Zeit, mich um Passwortsicherheit zu kümmern“ sind nicht selten Ursachen für fatale Folgen im Unternehmen. Sophos hat in seinem X-Ops' Active Adversary Report herausgefunden, dass im Jahr 2023 erstmals kompromittierte Zugangsdaten mit 56 Prozent die Hauptursache für Angriffe waren, die Datendiebstahl und/ oder Ransomware-Attacken zur Folge hatten. Das ist ein Anstieg von 26 Prozent von 2022 auf 2023.

Einfache aber wirkungsvolle Safer-Internet-Tipps für die Anwender
Neben einer guten Passwortpraxis ist es wichtig, „Nein“ zu sagen und die Angabe von Informationen zu verweigern. Nur weil eine Web-Applikation beispielsweise den Geburtstag oder andere augenscheinlich unwichtige Informationen wissen möchte, heißt das noch lange nicht, dass diese Applikation die Informationen auch tatsächlich braucht oder gar ein Recht darauf hat. Was im Internet nicht preisgegeben wird, kann weder weitergegeben noch missbraucht werden. Daher: Keine Angaben von noch so harmlosen Informationen und kein Anklicken von Links, die man nicht kennt oder benötigt. Zudem gilt es, keine fremden und potenziell gefährlichen Apps zu nutzen und die benötigten Apps immer auf dem neuesten Stand zu halten. Und grundsätzlich wäre die Standardeinstellung von Vorteil, dass alles was, man nicht kennt, potenziell als verdächtig oder bösartig behandelt wird, bis das Gegenteil bewiesen ist.

Safer-Internet-Tipps für Unternehmen
Firmen, die eine Website betreiben und vielleicht sogar Zahlungsdienste oder Customer-Management-Lösungen eingebunden haben, sollten diese auf Sicherheit überprüfen. Wenn die dafür benötigten Ressourcen oder Fachkenntnisse nicht ausreichen, bieten sich externe

Experten an, welche unabhängig prüfen, was gut eingerichtet und gesichert ist und welche Sicherheitsprobleme dringend behoben werden müssen. Denn eines ist sicher: Cyberkriminelle testen teils hoch automatisiert die Sicherheit jedes Servers und jeder Webseite auf Schwachstellen.

Viele Menschen, die früher bei der Arbeit das Internet nutzten, um nur Nachrichten zu lesen oder E-Mails abzurufen, verwenden es jetzt täglich auf vielfältige Weise – auch um mit Kollegen zusammenzuarbeiten, die sie vielleicht weniger gut oder gar nicht kennen. Diese heute weitgehend übliche Arbeitsweise öffnet Cyberkriminellen Tür und Tor für Betrugsmaschen und Social Engineering. Darum sollen Unternehmen Ihre Mitarbeiter regelmäßig zu den aktuellen Gefahren und vor allem zum sicheren Verhalten im Internet schulen. Es ist wichtig, dass sie eigenständig Betrugsversuche erkennen, diesen nicht folgen und an die entsprechenden internen Stellen melden.

Klassische Security ist gut, reicht aber nicht aus. Cyberkriminelle verfügen über Mittel und Tools, Schwachstellen auszunutzen, die sie beispielsweise in unbekannten Netzwerk- und IoT-Geräten oder in der IT-Lieferkette entdecken. Eine hohe Sicherheit ist dann möglich, wenn sämtliche Security-Lösungen in einem intelligenten und KI-gestützten Ökosystem eingebunden und kontinuierlich mit menschlicher Expertise kombiniert werden. Security Services, welche mit Threat Hunting die schnelle Reaktion auf Verdachtsfälle oder Angriffe garantieren, helfen den Schaden durch Cyberkriminelle rechtzeitig abzuwehren.

Vertrauen ist gut, Kontrolle ist besser
Nahezu kein Unternehmen kann sich heute noch auf die Sicherheit innerhalb traditioneller IT-Perimeter verlassen. Das eine Unternehmensnetzwerk gibt es nicht mehr. Viel mehr überspannt das Netzwerk weite Bereiche des Internets, darunter die Cloud und die gesamte IT-Lieferkette oder SaaS-Dienste. Dem sollten Unternehmen mit einer erweiterten Strategie Rechnung tragen und nach Lösungen suchen, die weit mehr als nur die eigenen Server und Arbeitsplätze mit Firewalls und Endpoint-Schutz absichern. Zero Trust-Methoden und Network Detection and Response (NDR) in Verbindung mit hochgradig spezialisierten externen Security-Services, werden diesen neuen Anforderungen gerecht.

In diesem Sinne: Happy Safer Internet Day!

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de