Cybercrime – kein Ende in Sicht

Ende Jahr schaut man gerne zurück, was war und blickt in die Zukunft, was kommt auf uns zu. Auch im Security-Bereich ist dies nicht anders. Ein Virus hat uns dabei in Atem gehalten. Nicht nur für den Menschen waren Viren eine Bedrohung, auch auf dem Computer wüten diese.

Gefahren im Auge behalten.

Während des Lockdowns arbeiteten viele Angestellte von zu Hause aus. Die meisten Firmen traf diese neue Arbeitsweise auf dem falschen Fuss. Von einem Tag auf den anderen mussten entsprechende Mittel zur Verfügung gestellt werden. Dabei war die Sicherheit oft nicht die erste Priorität. Es musste, verständlicherweise, die Erfüllung der Dienstleistung sichergestellt werden. Die Hacker nahmen auf diesen Umstand jedoch keine Rücksicht und erhöhten sogar ihre Angriffe.

So verzeichnete MELANI, die Melde- und Analysestelle Informationssicherung, neu Nationales Zentrum für Cybersicherheit in ihrem ersten Halbjahresbericht 2020 rund 230 gezielte Malware-Angriffe in der Schweiz, davon 42 Ransomware-Attacken. Bei Ransomware werden alle erreichbaren Dateien verschlüsselt und nur gegen Bezahlung eines Lösungsgelds können diese wiederhergestellt werden. Fast wöchentlich konnte in den Tageszeitungen von erfolgreichen Angriffen gelesen werden. Dabei kam es in mindestens einem Fall sogar zur Insolvenz des Unternehmens.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Hoher Schaden durch Cyberkriminelle

Gleichzeitig wurden im vergangenen Jahr 3000 neue Phishing-Seiten entdeckt, die Dunkelziffer ist sicherlich massiv höher. Bei Phishing geht es darum, den Menschen dazu zu bringen, einen Link anzuklicken. Entweder wird dann gleich ein Schädling auf dem eigenen Rechner installiert oder es wird versucht, an Kreditkarten-Informationen zu gelangen.

Dass dies sehr erfolgreich ist, zeigen die simulierten Angriffe, die wir durchführen dürfen. Trotz mehrerer Hinweise fallen zwischen 40 und 70 Prozent der angeschriebenen Personen auf die Fälschung herein und klicken auf den Link. Bei bestimmten Szenarien geben viele sogar ihr Passwort bekannt. Dies kann für ein Unternehmen fatale Folgen haben, sollten diese Zugangsdaten auch von aussen nutzbar sein, zum Beispiel für den Zugriff auf die E-Mails. Sollte der Angreifer mal im Firmen-Netzwerk sein, ist er kaum mehr aufhaltbar.

Eine Studie von McAfee und dem Centre for Strategic & International Studies wurde der Schaden im Jahr 2017 durch Cyberkriminellen auf $ 600 Milliarden geschätzt. Als Vergleich geht die UN beim weltweiten Drogenhandel von $ 320 Milliarden aus. Also beinahe doppelt so viel machen Cyber-Angriffe aus.

Nach der Umstellung auf das Home-Office kam es zu verstärkten Cyberangriffen auf Unternehmen. Die KPMG führte daher zusammen mit Harvey Nash eine Umfrage bei 4200 CEOs durch. Bei 90 Prozent der Unternehmen mussten Mitarbeitende von zu Hause aus arbeiten. Viele rechnen damit, dass dies auch nach dem Lockdown so bleiben wird. Während des ersten Lockdowns im Frühling 2020 verzeichneten diese Unternehmen eine sprunghafte Zunahme der Angriffe um über 40 Prozent. Die Zahlen für das Jahr 2020 dürften sicherlich nochmals höher liegen. Ein lukratives Geschäft also.

Letztes Jahr stand klar Malware im Fokus. Einer dieser Schädlinge ist Trickbot. Sobald er sich in einem Gerät einnisten konnte, kommuniziert er mit seinem Erbauer. Dieser kann nun den PC fernsteuern, weitere Malware installieren, Spam verschicken oder ein Unternehmen angreifen. Damit er nicht auffällt, verändern die Erbauer diesen ständig. Durchschnittlich alle 6,5 min. wurde von Trickbot ein neues Sample veröffentlich und damit versucht unerkannt Computer und Netzwerke zu infiltrieren. Die Möglichkeiten von Trickbot reichen von Ausspähen von Passwörtern, das Auslesen von vertraulichen Daten bis hin zum Löschen der Daten oder Verschlüsselung dieser. Aber auch die Gegenmassnahmen lassen nicht auf sich warten. So hat Microsoft Anfang 2020 69 der kontrollierenden Server ausschalten können. Doch wie bei Fuchs und Hase wurden diese sehr schnell wieder ersetzt. So berichtete Microsoft Ende Oktober in einem Blog-Beitrag, dass sie 120 von 128 Server der Infrastruktur ausser Betrieb nehmen konnten. Damit ist das «Spiel» aber nicht gewonnen.

Software regelmässig aktualisieren

Für das neue Jahr gilt es, diese Gefahren weiter im Auge zu behalten. Diese werden garantiert weiter zunehmen. Zu Lukrativ ist dieses Businessmodell. Zu den Gegenmassnahmen gehört an erster Stelle ein aktuelles Antivirenprogramm. Wie beschrieben reicht es heute nicht mehr, dieses nur einmal pro Tag zu aktualisieren, viele Antiviren-Firmen bieten alle Stunde ein Update an. Dieses gilt es möglichst schnell zu installieren. Idealerweise erfolgt dies automatisch. Von Hand ist dies nicht mehr zu bewältigen. Aus Erfahrung kann es sein, dass trotz eingestelltem Automatismus das Programm nicht auf dem aktuellen Stand ist. Daher gilt es für die IT, alle Geräte regelmässig manuell zu überprüfen. Nebst dem Antivirenprogramm gilt es aber auch die installierte Software regelmässig zu aktualisieren, nicht nur das Betriebssystem.

Neben der Technik gilt es insbesondere 2021 die Mitarbeitenden mit an Bord zu holen. Nur was bekannt ist, kann auch gelebt werden. Regelmässige Sensibilisierungen sind für die Sicherheit von grosser Bedeutung. Dabei sollte die Durchführungsart angepasst werden, von Schulungen, Informationen per E-Mail und auf dem Intranet, Videos, Bildern, aber auch einmal ein simulierter Angriff. Verschiedene Variationen erhöhen das Bewusstsein und die Nachhaltigkeit. Nicht vergessen werden darf, schon nur ein Klick eines Mitarbeitenden genügt und der Schädling breitet sich im Netzwerk aus.

Nur das Zusammenspiel Mensch und Technik verhindert einen erfolgreichen Angriff. Auch wenn die Angreifer raffinierter und ihre Werkzeuge besser werden, mit einem wachsamen Auge bleiben die Firmendaten auch im neuen Jahr vor fremden Blicken verschont.