Serie Cyber-Sicherheit

Kein Lösegeld zahlen

[20.12.2022] Nur wer seinen Gegner versteht, kann die richtigen Gegenmaßnahmen einleiten. Im dritten Teil unserer Serie geht es darum, wer die Cyber-Kriminellen sind und welche Methoden sie anwenden.

Der Begriff Hacking bezeichnet die Manipulation eines Systems mit dem Ziel, dieses dazu zu bringen, etwas zu tun, wozu es ursprünglich nicht gedacht war. Bei Hackern mit kriminellen Absichten spricht man von Cyber-Kriminellen, von Black-Hat-Hackern oder kurz Black-Hats. Daneben gibt es noch Hacktivisten, die durch Cyber-Angriffe auf ihre gesellschaftspolitischen Ziele aufmerksam machen wollen.
Es gibt auch gute Hacker: White-Hat-Hacker, Ethical Hacker oder Cybersicherheitsforscher. Das sind Personen, die als Aktivisten oder im Auftrag von Einrichtungen und Unternehmen Sicherheitslücken aufspüren. Werden sie fündig, informieren sie das Unternehmen oder die Einrichtung über die Schwachstellen.
Für die meisten Cyber-Kriminellen geht es nur um eins: Geld. Anstatt mit einem genialen Solisten hat man es meist mit kriminellen Unternehmensstrukturen zu tun. Die möglichen Lösegeldsummen gepaart mit geringen Aufklärungsquoten ergeben ein lukratives kriminelles Geschäftsfeld. Ob festangestellt im Großraumbüro einer großen Hacker-Gruppierung oder als selbstständiger Auftragshacker – heutzutage wird arbeitsteilig gearbeitet. Übersetzer verfassen Texte für Phishing-E-Mails, Programmierer schreiben Schad-Software, andere pflegen den Auftritt im Darkweb. Einzelne Dienstleistungen lassen sich für wenig Geld einkaufen (Crime as as Service). Hierzu gehört auch die benötigte Schad-Software. Die häufigsten Angriffsmethoden sind:

Phising

Phishing: Beim Phishing (abgeleitet von fishing = angeln) versuchen Cyber-Kriminelle das Opfer dazu zu bringen, Zugangsdaten preiszugeben oder Schad-Software zu installieren. Hierzu nutzen sie E-Mails, falsche Websites sowie SMS oder Messenger-Dienste (so genanntes Smishing, von SMS und Phishing). Die Nachrichten enthalten entweder mit Schad-Software präparierte Anhänge oder Links auf Internet-Seiten, auf denen Zugangsdaten eingegeben werden sollen. Oftmals sind sie von echten E-Mails oder Websites nicht zu unterscheiden. Aufwendiger wird es, wenn gezielt ein Opfer ausgewählt wurde. Durch Recherche in sozialen Netzwerken werden auf Schwachstellen der Person abgestimmte E-Mails verschickt (Spearphishing). Phishing-Nachrichten bedienen sich aller Methoden des Social Engineerings, psychologischer Manipulation, die das Opfer dazu bringen, unüberlegt zu handeln. Es bleibt damit auch für Personen gefährlich, die gut informiert sind.
Bei ungewöhnlichen E-Mails sollte immer kontrolliert werden, ob der angezeigte Absender und die E-Mail-Adresse übereinstimmen. Ein Rückruf bei dem vermeintlichen Absender, etwa der Bank oder dem Kollegen, hilft, die Nachricht zu verifizieren. Hierzu sollten niemals die Kontaktinformationen auf der durch den Link aufgerufenen Internet-Seite genutzt werden. Erfolgreiche Phishing-Vorfälle müssen schnell gemeldet und Passwörter aktualisiert werden, insbesondere das Passwort des E-Mail-Accounts und die Zugangsdaten zum System. Wurde das erbeutete Passwort mehrfach verwendet, müssen alle Verwendungen geändert werden.

Identitätsdiebstahl und Ransomware

Identitätsdiebstahl: Gelangt der Cyber-Kriminelle durch Phishing oder das Knacken einfacher Passwörter an Zugangsdaten, kann er die Identität des Opfers übernehmen und in dessen Namen Straftaten verüben oder die Identität an andere Kriminelle verkaufen. Einen Schutz bietet hier eine Mehrfaktor-Authentisierung. Viele Dienstleister bieten mittlerweile Zwei-Faktor-Authentisierung an. Um Zugang zu erlangen, werden zwei festgelegte Komponenten benötigt, die Zugangsdaten und ein Gegenstand, beispielweise ein Smartphone, auf das ein Einmalcode geschickt wurde oder eine TAN.
Ransomware: Bei Ransomware handelt es sich um Schad-Software, welche Daten und Systeme verschlüsselt. Gegen Zahlung eines Lösegelds versprechen Cyber-Kriminelle die Entschlüsselung. Die Lösegeldzahlung garantiert weder die versprochene Entschlüsselung noch, dass keine Schad-Software auf dem System verbleibt. Auch ein erneuter Angriff lässt sich so nicht ausschließen. Da viele Betroffene dennoch zahlen, sind Ransomware-Angriffe für die Kriminellen lukrativ. Wird die Lösegeldzahlung verweigert, drohen Cyber-Kriminelle nach einem Ransomware-Angriff oft mit der Veröffentlichung gestohlener Daten, um das Opfer doch noch zum Zahlen zu bewegen. Auch wenn die Lösegeldforderung erfüllt wird, landen die gestohlenen Daten oft im Darkweb. Kriminellen kann man nicht vertrauen. Ransomware und andere Schad-Software können sich auch über Geschäftspartner und Dienstleister verbreiten. Die Zahl dieser Angriffe auf die Lieferkette nehmen zu. Besonders Attacken auf IT-Dienstleister, die sich von dort auf die Systeme der Kunden ausbreiten, können große Schäden anrichten. Die wirkungsvollste Gegenmaßnahme sind regelmäßige Sicherungskopien (Back-ups). So wird der Datenverlust verringert und die Kommune ist schneller wieder einsatzfähig. Um diese Angriffsart für Cyber-Kriminelle unattraktiv zu machen, sollte man keine Lösegeldzahlungen leisten.

Staatliche Akteure

Staatliche Akteure und APT-Gruppen: Im Kontext des russischen Angriffskriegs auf die Ukraine rückten staatliche Akteure vermehrt in das Bewusstsein der Öffentlichkeit. Zu diesen gehören Internet-Trolle und Propagandisten ebenso wie Geheimdienste, regierungsnahe Gruppierungen und APT-Gruppen, die sich Zugang zu Systemen verschaffen. APT steht für Advanced Persistent Threat und beschreibt Gruppen, von denen eine fortgeschrittene, andauernde Bedrohung ausgeht. Internet-Trolle verbreiten Desinformationen im Internet und auf Social-Media-Plattformen. Ziel ist es, den Rückhalt der Regierung in der Bevölkerung zu schwächen und den sozialen Frieden zu stören.

()

Das Hessen CyberCompetenceCenter (Hessen3C)
Dieser Beitrag ist in der Ausgabe Dezember 2022 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Hessen CyberCompetenceCenter, Serie Cyber-Sicherheit