Zunehmende Cyberkriminalität

Welche Gegenmaßnahmen sind sinnvoll und helfen wirklich?

© AdobeStock_57159281, Adobe Stock, santiago silver

Ransomware, Malware, Phishing und DoS-Attacken. Tagtäglich sehen sich Unternehmen, Organisationen und Einzelpersonen vielfältigen Cyberangriffen ausgesetzt und die Bedrohungslage nimmt laut BSI Lagebericht 2021 stetig zu. Die Liste möglicher Angriffsszenarien ist zwar übersichtlich, aber auch lang. Um allen Betroffenen eine bestmögliche Sicherheit zu gewährleisten, bedarf es ständig überprüfter und regelmäßig angepasster IT-Security-Maßnahmen. Denn IT-Sicherheit ist kein anhaltender Zustand, sondern ein fortlaufender, kontinuierlich an veränderte Bedrohungsszenarien und Angriffsvektoren anzupassender, Prozess.

Vor dem Hintergrund des Russland-Ukraine-Konflikts warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) wiederholt vor einem erhöhten Risiko durch gezielte Cyberangriffe. Insbesondere Unternehmen, die unter die KRITIS-Verordnung fallen, sind gefährdet. Es kommt daher nicht von ungefähr, wenn die englische Sprache für diese Art der Kriegsführung mit Viren, Würmern und Trojanern oftmals den Begriff „Code War“ verwendet. Der Wettstreit zwischen Gut und Böse gleicht einem Hase-Igel-Wettlauf, bei dem sowohl Cyberkriminelle als auch Cyberabwehr-Experten versuchen, die Nase vorne zu haben. Beide Seiten entwickeln immer wieder geeignete Angriffs- und Verteidigungsstrategien.

Wertvolle Informationen erbeuten

Cyberangriffe haben für Hacker sowie für wirtschaftlich oder politisch motivierte Institutionen einen entscheidenden Vorteil: Um wertvolle Informationen und Geschäftsgeheimnisse zu stehlen, muss heutzutage nicht mehr in gesicherte Gebäude eingebrochen werden. Cyberkriminelle können aus sicherer Entfernung „im oder durch den Cyber-Raum“ ihren Angriff virtuell durchführen. Während gegen staatliche Akteure oft „kein Kraut gewachsen ist“, haben gewöhnliche Hacker zu viele Gegner, um lange unerkannt zu bleiben.

Vielfältige Cyberangriffe durch Malware

Malware – zu Deutsch Schadsoftware – ist der Sammelbegriff für „bösartige“ Programme und Software, die nur einem Zweck dienen: Nutzern teils beträchtlichen Schaden zuzufügen! Egal ob Viren, Würmer, Trojaner oder Ransomware, alle Unterarten verfolgen ein Ziel: Unternehmen und Einzelpersonen zu schaden! Dabei arbeitet jede Schadsoftware anders.

Computerviren

haben meist einen hochgradig destruktiven Charakter. Es handelt sich dabei um einen Programmcode, der sich an eine Wirtsdatei andockt, das Betriebssystem infiltriert und sich dort selbstständig vermehrt. Sie verhindern die Ausführung von Betriebssystemen und Applikationen, infizieren oder löschen Dateien, beschädigen Hardware-

© AdobeStock_65982251, ©Adobe Stock, weerapat1003

Autor:
Robert Korherr,
Geschäftsführer
ProSoft GmbH
www.prosoft.de

© AdobeStock_169435664, Adobe Stock, arrow

© AdobeStock_428658994, Adobe Stock, Dzmitry

Komponenten und machen diese nutzlos. Viren hängen sich vornehmlich als Payload an Dateien an oder geben vor, eine harmlose Datei (Datei-Spoofing) zu sein.

Computerwürmer

Eine andere Bedrohung stellen Computerwürmer dar. Im Gegensatz zu Viren befallen sie meist keine Programme, sondern vornehmlich Speichermedien. Sie arbeiten zwar ähnlich wie ein Virus, aktivieren sich jedoch vollkommen selbstständig. Ohne Nachladen weiteren Schadcodes ist das Risiko von Würmern jedoch eher gering. Lediglich wenn ein eingeschleuster Wurm Schadcode nachladen kann, nimmt das Risiko zu.

Ransomware

Hinter klassischen Viren steckt oft eine rein politische Motivation, beispielsweise wenn Anlagen sabotiert werden sollen, wie 2010 mit dem Computerwurm Stuxnet. Immer häufiger sind jedoch auch monetäre Ziele zu beobachten: Die finanzielle Bereicherung durch das „Abfischen“ von Zugangsdaten, das Umleiten von Zahlungsströmen und die Erpressung von Lösegeld (englisch: Ransom). Ransomware ist auf dem Vormarsch! Laut Global Threat Intelligence Report von NTT erreichte Ransomware bis Ende 2021 einen Anteil von zwölf Prozent bezogen auf alle Malware-Angriffe. Alleine zwischen 2017 und 2021 wurden dabei Schäden in Höhe von ca. 20 Milliarden US-Dollar verursacht. Ransomware verhindert den Systemzugang und/oder verschlüsselt wichtige Daten. Für die Wiederfreigabe verlangen die Erpresser von den Opfern Lösegeld, das diese oft mit Kryptowährung zahlen müssen. Der Umgang mit Ransomware-Angriffen ist heikel. Man kann nicht sicher sein, dass das System nach Lösegeldzahlung auch tatsächlich wieder freigegeben wird.

© AdobeStock_536033828, Adobe Stock, dizain

Welche Strategie bietet zuverlässigen Schutz vor Malware?

Die nachweislich beste Abwehr von Malware bietet – wen wundert's – eine zuverlässige Anti-Malware-Lösung. Doch wie erkennt man Malware? Jede Malware hat ein eindeutiges Muster, eine Viren-Signatur. Sobald eine neue Signatur bekannt ist und der Anti-Malware-Hersteller sie in der Blacklist seiner Software ergänzt hat, sind die Nutzer auf der sicheren Seite. Heuristik, also die Fähigkeit, Vorhersagen aufgrund von Wahrscheinlichkeiten zu treffen, hilft bei der Identifizierung neuer Schadsoftware. Bei täglich knapp 400.000 neuen Malware-Varianten (BSI Lagebericht IT-Sicherheit 2021) stoßen die Anti-Malware-Hersteller jedoch an ihre Grenzen. Hier hilft die Bündelung von mehreren Anti-Malware-Engines in einer einzigen Lösung. Durch Anti-Malware-Multiscanner entsteht eine Schwarmintelligenz, die Erkennungsraten von bis zu 99,9 Prozent ermöglicht. Darüber hinaus bestehende Restrisiken, beispielsweise durch Zero-Day-Malware, lassen sich durch Datei-Desinfektion eliminieren. Datei-Desinfektion geht davon aus, dass jede Datei, in die sich Malware einbetten lässt, auch Schadcode enthält und desinfiziert diese Daten. Riskante Dateiformate werden in risikolose Dateitypen umgewandelt, ohne die Funktion zu beeinflussen. Das Risiko, Opfer von Cyberkriminalität zu werden, lässt sich so bereits deutlich reduzieren.

Brute-Force-Attacken

(von englisch „rohe Gewalt“) sind wie die Brechstange bei Einbrüchen. Nach dem Prinzip „Versuch und Irrtum“ wollen Cyberkriminelle mittels rechenleistungsstarker Computer und automatisierter Tools die richtige Kombination aus Name und zugehörigem Passwort ihrer Opfer knacken. Bei dieser Angriffsmethode sollen Zugänge durch wiederholte Eingabe von möglichen Nutzer-Passwort-Kombinationen aufgebrochen

© AdobeStock_550072336, Adobe Stock, Monti

© AdobeStock_553004015, Adobe Stock, Maksym Yemelyanov

werden. Immer leistungsfähigere Computersysteme und Passwörter, die meist schwach und vielfach auch noch für weitere unterschiedliche Accounts verwendet werden, machen Brute-Force-Attacken zum lohnenden Geschäftsmodell.

Man-in-the-Middle-Angriffe

Durch Man-in-the-Middle-Angriffe versuchen Cyberkriminelle als Mittelstation an einer Kommunikation zwischen Sender und Empfänger teilzunehmen. Bei dieser Form von Cyberkriminalität werden Kommunikationsinhalte mitgelesen oder manipuliert, indem sich Angreifer gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgeben. Auf diese Weise kann der Man-in-the-Middle auch Zugangsdaten ausspionieren und verwerten.

Phishing

als Betrugsversuch zielt frontal auf das schwächste Glied in jeder Abwehrkette, den Menchen. Gut gefakte E-Mails mit einer Handlungsaufforderung von bekannten Absendern, wie etwa der eigenen Hausbank, führen oft dazu, dass ein Empfänger seine Zugangsdaten auf einer ebenfalls gefakten Webseite leicht preisgibt. Cyberkriminelle versenden solche gefakten Nachrichten willkürlich an eine Vielzahl von E-Mail-Accounts, in der Hoffnung, dass einige Empfänger auf diese E-Mail reinfallen, diese für „echt“ halten und wie vom Angreifer gewollt, entsprechend reagieren. Die wenig schöne Überraschung dieses nicht gezielt auf einzelne Empfänger ausgeführten Angriffs ist meist ein leeres Bankkonto.

Spear-Phishing hingegen ist eine Betrugsvariante, die sich gezielt an bestimmte Personen oder Organisationen richtet. Die Opfer werden dabei über Wochen und Monate gezielt ausspioniert, Gewohnheiten und Präferenzen in Erfahrung gebracht und ein individuelles Persönlichkeitsprofil erstellt. Auf Basis der gesammelten Daten lassen sich maßgeschneiderte, personenbezogene Phishing-Angriffe realisieren. Die hohe Glaubwürdigkeit der Angriffe optimiert die Erfolgsquote dieses Betrugsversuchs für Cyberkriminelle.

Schutz vor den Folgen gestohlener Identitäten

Über Phishing, Brute-Force- und Man-in-the-Middle-Attacken gestohlene Anmeldeinformationen sind bei Logins, die durch eine Zwei-Faktor-Authentifizierung (2FA) beziehungsweise eine Mehr-Faktor-Authentifizierung (MFA) geschützt werden, nutzlos. Die FIDO-Alliance hat mit FIDO2 sogar einen Login-Standard entwickelt, der überhaupt kein Passwort benötigt und trotzdem extrem sicher ist. Dazu ist der Faktor „Haben“ in Form eines Hardware Token Voraussetzung. Ein realistisches Restrisiko gestohlener Identitäten bleibt für den Nutzer, sofern er die identische Kombination aus Benutzername und Passwort auch für andere Accounts verwendet, die nur statische Anmeldeinformationen voraussetzen.

Erhöhte Gefahr durch DoS- und DDoS-Attacken

Denial of Service Angriffe (DoS) und Distributed Denial of Service Angriffe (DDoS) sind nicht neu, doch als Angriffsmethode immer noch gebräuchlich. Insbesondere in Jahreszeiten mit umsatzstarken Onlineaktivitäten im E-Commerce-Bereich (Black Friday, Cyber Monday, Vorweihnachtsgeschäft, Weihnachtsgeschäft) beobachtet das BSI einen Anstieg solcher Aktivitäten. Beim Versuch, vorhandene Systeme mit einer Vielzahl von Anfragen zu überlasten und damit außer Betrieb zu setzen, gibt es unterschiedliche Formen des Angriffs, wie beispielsweise Syn-Flooding, Ping-Flooding und Mail-Bombing. Der Schaden liegt bei allen Angriffsmethoden in der zeitweisen Nichtverfügbarkeit der IT-Systeme. Einige Unternehmen mögen dies verschmerzen können, doch für einen Online-Shop-Betreiber ist so eine koordinierte Attacke mitunter existentiell. Bis zur Wiederherstellung der Verfügbarkeit seines Shops können keine Online-Bestellungen abgewickelt und somit kein Geld verdient werden. Neben dem immensen finanziellen Schaden ist zudem die Reputation des Online-Shops bei mehrfacher Nichtverfügbarkeit ebenfalls beträchtlich beschädigt.

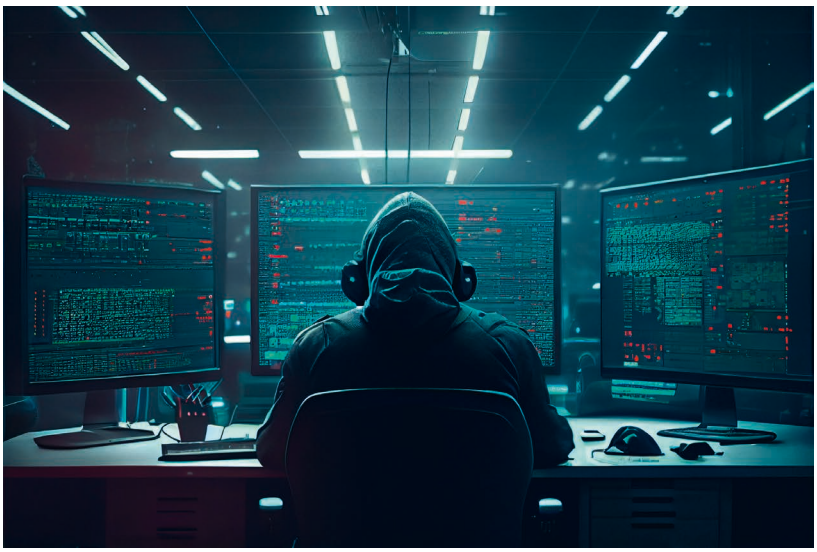
Schutz vor DoS / DDoS

Einige der DoS-Angriffe nutzen Bugs und Sicherheitslücken gezielt aus. Patch-Management, also das zeitnahe Verteilen von Sicherheitsupdates, schützt allgemein vor Cyberangriffen. Außerdem lassen sich Angriffsflächen vermeiden, indem man verhindert, dass Web-Applikationen Zugriff auf Ports, Protokolle oder Applikationen erhalten, die für eine Kommunikation im größeren Umfang nicht ausgelegt sind. Dabei kann es sehr hilfreich sein, die Infrastruktur hinter CDN (Content Distribution Network) oder einem Load-Balancer zu platzieren, denn dies kann die Datenmengen zwischen Front- und Backend begrenzen.

Fazit

Gegen die üblichen Verdächtigen bei Cyberangriffen schützen die üblichen Verdächtigen in der Cyberabwehr:

- Anti-Malware-Multiscanner plus Datei-Desinfektion bieten angesichts der hohen Anzahl täglich neuer Malware-Varianten den bestmöglichen Schutz, auch vor Zero-Day Attacken.
- Die Angst vor gestohlenen Identitäten verliert ihren Schrecken durch die Absicherung mit einer Zwei- oder Mehr-Faktor-Authentifizierung.
- Bei DoS oder DDoS Angriffen ist die Verkleinerung der Trefferfläche und die Entkoppelung von Front- und Backend sehr wirkungsvoll. ◄



© AdobeStock_564803102, Adobe Stock, marikova