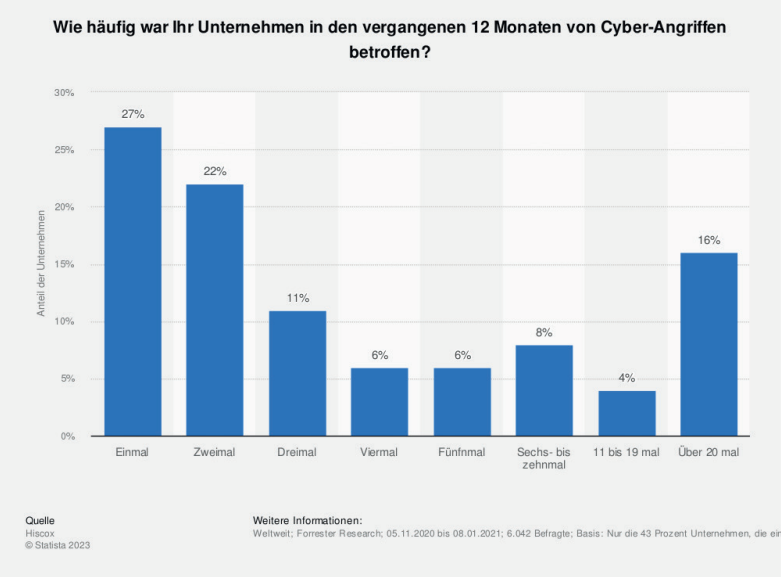
IT-SECURITY STORIES

1 Anatomie eines Hackerangriffs

Hackerangriffe auf IT-Infrastrukturen von Unternehmen sind heutzutage ein wiederkehrendes Problem. Sowohl große Konzerne als auch kleine und mittelständische Unternehmen sind betroffen. Die Täter hinter Ransomware-Angriffen versuchen, Daten zu stehlen und von den infizierten Unternehmen Lösegeld zu erpressen. Die gestohlenen Daten werden entweder für weitere Angriffe genutzt oder verkauft. Aufgrund von „Ransomware as a Service" (RaaS), einer Dienstleistung, die die Nutzung von Ransomware erleichtert und künstliche Intelligenz integriert, können solche Angriffe heutzutage von weniger spezialisierten Angreifern durchgeführt werden. Der Anstieg solcher Angriffe in letzter Zeit ist auf solche Dienstleistungen zurückzuführen.



Zugang zum Netzwerk

Der typische Ablauf der meisten Angriffe ist ähnlich, jedoch können sich die Methoden leicht unterscheiden. Der Angreifer versucht zunächst, Zugang zum Netzwerk zu erhalten. Je wertvoller das Ziel ist, desto professioneller geht er vor.

Wenn der einfache Zugang nicht gelingt, indem Schwachstellen in Software oder Hardware ausgenutzt werden, versucht der Angreifer, sich durch Phishing-Angriffe Zugang zum Netzwerk zu verschaffen. Während viele Unternehmen mit breit angelegten Phishing-Angriffen bombardiert werden, werden besondere Ziele wie Vorstandsmitglieder oder Teamleiter mit ausgefeilten Spear-Phishing-Angriffen attackiert.

Tipp: Es ist entscheidend, das Bewusstsein der Mitarbeiter zu schulen. Durch geeignete Schulungen und Maßnahmen können Phishing-E-Mails im Ernstfall schneller erkannt und somit das Angriffsrisiko verringert werden.

Ausweitung der Rechte

Wenn der Angreifer trotzdem Zugang zum Zielsystem erhält, versucht er schrittweise seine Rechte im Netzwerk auszuweiten, um die Kontrolle zu übernehmen. Der Angreifer nutzt dabei Schwachstellen im internen Netzwerk, aufspürbare Zugangsdaten und unzureichendes Rollen- und Rechte-Management.

Tipp: Einfache Maßnahmen erschweren dem Angreifer bereits die Ausweitung seiner Rechte. Das ungesicherte Speichern von Zugangsdaten als Textdatei sollte vermieden werden. Stattdessen sollte ein Passwort-Safe verwendet werden. Ein funktionierendes Rollen- und Rechte-Management ist ebenfalls wichtig, um die Bewegungsfreiheit und den Zugriff der Benutzer einzuschränken. Durch regelmäßige Schwachstellen-Scans und ein Patchmanagement können verwundbare Komponenten identifiziert und Maßnahmen zur Minimierung des Angriffsrisikos abgeleitet werden.

Kopieren der Daten

Nachdem der Angreifer das Netzwerk erkundet und seine Rechte ausgeweitet hat, kopiert er die Daten. Besonders Konversationsdaten wie E-Mails oder Chat-Verläufe sind interessant, um weitere Angriffe auf andere Unternehmen zu starten. Auch geistiges Eigentum, Entwicklungs- und Forschungsdaten können verkauft werden. Finanzdaten sind für Angreifer vor allem für die Liquiditätsanalyse und zur Festlegung des Lösegeldbetrags von Interesse. Sobald die relevanten Daten kopiert wurden, verschlüsselt der Angreifer sie innerhalb des Netzwerks, um eine Erpressung zu starten.

Die Verschlüsselung erfolgt nach den gleichen Prinzipien wie bei jeder anderen geschäftlichen Verschlüsselung. Die Größe des Datenbestands, der verschlüsselt werden muss, sowie die Komplexität der Verfahren und der Schlüssellänge haben Auswirkungen auf die benötigte Rechenleistung.

Tipp: Eine Monitoring-Lösung mit Last- und Ressourcenüberwachung kann alarmieren, wenn ein Verschlüsselungsprozess ungewöhnlich viele Ressourcen beansprucht oder unbekannte Prozesse gestartet werden. Zentrales Speichern und Auswerten von Logdateien ist ebenfalls wichtig, um verdächtige Aktivitäten im Netzwerk zu erkennen, die auf die Vorgehensweise von Angreifern hinweisen könnten. Ein zentrales Logging hilft nicht nur bei der Analyse des Angriffsverlaufs, der Identifizierung betroffener Systeme und der Ermittlung des Datenverlusts, sondern ist auch für ein Security Information and Event Management (SIEM) unverzichtbar.

Wenn ein laufender oder abgeschlossener Angriff erkannt wird, ist schnelles Handeln erforderlich, um den Geschäftsbetrieb aufrechtzuerhalten. Jeder Mitarbeiter im Unternehmen sollte über die notwendigen Prozesse und seine Befugnisse informiert sein. Neben der Dokumentation aller relevanten Bereiche ist regelmäßiges Training von Vorteil.

Studien von verschiedenen Branchenverbänden zeigen, dass die finanziellen Forderungen der Angreifer nur einen Bruchteil der Gesamtkosten eines Angriffs ausmachen. Die tatsächlichen Verluste liegen oft um ein Vielfaches höher. Der Verlust von geistigem Eigentum und Reputation lässt sich nur schwer quantifizieren.

Um die Kosten im Falle eines Vorfalls gering zu halten, können präventive Maßnahmen ergriffen werden. Der Aufbau einer sicheren IT-Infrastruktur ist von großer Bedeutung. Redundanzen und Firewalls allein reichen heute nicht mehr aus. Die Einrichtung eines Krisen- und Notfallmanagements sowie eines Business Continuity Managements sind entscheidend. Eine sicherheitsorientierte Unternehmenskultur kann durch Awareness-Schulungen und die Etablierung einer Fehlerkultur erreicht werden, bei der nicht die Schuldigen im Vordergrund stehen, sondern die Frage, wie Fehler vermieden werden können.

Cyberangriffe sind eine dauerhafte Bedrohung für Unternehmen. Während die Kosten eines erfolgreichen Angriffs schwer abzuschätzen sind (IT-Kosten, Public Relations, Produktionsausfall, Wiederbeschaffung, Vertragsstrafen, erhöhte Versicherungsprämien, Rechtsberatung), können die Kosten für präventive Maßnahmen zur Stärkung der IT-Sicherheit besser geplant und erfasst werden.