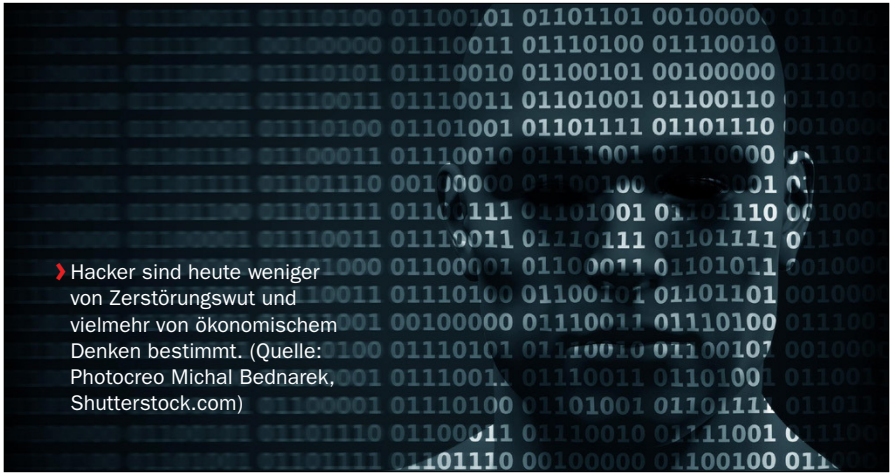
Cyberkriminalität: Abwehrstrategien gegen neue Bedrohungsszenarien

Cyberkriminalität hat sich zu einem riesigen Geschäft mit eigener Wertschöpfungskette entwickelt. Dieser Artikel liefert einen Ausblick auf die Weiterentwicklung der Bedrohungslage, Cyberangriffen und möglichen Abwehrstrategien.

Cyberkriminalität hat sich über die Jahre zu einem wahren Geschäfts- und Erfolgsmodell etabliert. Aufgrund von Spezialisierung und Arbeitsteilung haben sich sogar Wertschöpfungsketten entwickelt. Angriffe werden heutzutage sowohl genauer gezielt als auch breiter gestreut, je nachdem ob politische oder monetäre Aspekte im Vordergrund stehen.



› Hacker sind heute weniger von Zerstörungswut und vielmehr von ökonomischem Denken bestimmt. (Quelle: Photocreo Michal Bednarek, Shutterstock.com)

Es gibt deutlich mehr Attacken, neue Botnetze, neue Vektoren und vor allem mehr Aggressivität. Während vermehrt Massenangriffe durch DDoS-Attacken auf Systeme und Infrastrukturen gefahren werden, nimmt auch die Zahl der gezielten und manuellen Angriffe immer weiter zu – Cyberangriffe sind quasi Geschäftsmodelle, die weiterentwickelt werden, um Gewinne fortwährend zu maximieren bzw. Infrastrukturen zu stressen und Risiken minimal zu halten. Dabei ist Cyberkriminalität auf das Ausschöpfen von Daten ausgelegt und hat sich eine Methodik der Schwachstellenidentifikation aufgebaut. Mittels verschiedenster Angriffsarten können so erhebliche Geldsummen generiert werden. Grundlage für diese Prozesse und Wertschöpfungsketten bieten die Unternehmensdaten bzw. personenbezogenen Daten.

Wer grundsätzlich davon ausgeht, dass ein Hacker direkt auch ein Cyberkrimineller ist, liegt allerdings falsch. Die folgende Abstufung zeigt, wie Hacker deklariert werden:

- Die **„White-Hats"** sind die „Guten" unter den Hackern. Sie bieten unter anderem ihr Wissen als Dienstleistung an und werden im Rahmen etwa von Penetrationstests in Unternehmen eingesetzt. Sie bewegen sich innerhalb des Gesetzes und halten sich an die Hackerethik.
- **„Grey-Hats"** bewegen sich innerhalb des gesetzlichen Grau- Bereichs und ein Stück weit darüber hinaus. Sie wollen in erster Linie nicht gegen die Hackerethik verstoßen, sind aber bereit einen gesetzlichen oder ethischen Verstoß in Kauf zu nehmen, um die eigenen Ziele zu erreichen. Dabei sind die „Grey-Hats" bestrebt, Sicherheitslücken ausfindig zu machen, damit diese behoben werden können.
- **„Black-Hats"** spiegeln die kriminelle Form des Hackertums wider. Ihr Ziel ist es vorwiegend, mit krimineller Energie an Daten zu kommen bzw. Infrastrukturen oder Systeme zu manipulieren und ggfs. zu infiltrieren.

Gerade weil es so viele Formen und digitale Dienste gibt, floriert das Geschäft des Hackens wie nie zuvor. Den Ursprung des klassischen Hackens findet man in den 70er Jahren, abgesehen von dem militärischen Ausspähen, welches schon deutlich früher stattgefunden hat. Mitte bzw. Ende der 70er Jahre haben die ersten Cracks Telefonsysteme „gehackt", um gratis zu telefonieren (phreaking) – Steve Jobs und Steve Wozniak haben sogar ein Gerät konstruiert und verkauft (Bluebox), mit dem es möglich war Telefonsysteme zu manipulieren. Auch Angriffe auf Banken gab es schon in den 80ern. Zudem gab es in dieser Zeit auch erste politische Hacks unter denen sich der Chaos Computer Club und vor allem Karl Koch einen Namen gemacht haben.

Mitte der 90er Jahre, mit Einführung der ersten Online-Shops und des drahtlosen Internets, haben Cyberkriminelle mit einfachem Passwort-Hacking und durchbrechen der Firewalls versucht manuell an Daten zukommen. Dabei stand der Reiz im Vordergrund, Sicherheitsbarrieren von Unternehmen zu durchbrechen, die zu dieser Zeit gewiss noch nicht so hoch waren, wie sie es heute sind. Durch technische Weiterentwicklungen und auch generell besser auf Sicherheit ausgelegte Systeme, dank Log File Management, Anti Viren Programmen, Intrusion-Detection / Prevention-Systemen etc., seitens der Security-Anbieter und der Unternehmen, ist auch das Hacken zunehmend anspruchsvoller geworden.

Mit den Jahren haben sich ganze Hacker-Geschäftsmodelle entwickelt. Durch die Trends wie Social Media, die Marktdurchdringung des Smartphones und Cloud Computing gibt es vielfältigere Angriffsziele und Wege. Die Abhängigkeit der Nutzer und Unternehmen von diesen Technologien macht es darüber hinaus attraktiver. Daher steigt die Bedeutung neuer und bestehender Angriffsmodelle. Diese erpressen (Ransomware), setzen Infrastrukturen außer Kraft, stehlen persönliche Daten

oder manipulieren Connected-Devices. Im ersten Schritt versuchen heutige Cyber-Kriminelle ein auserspähtes Unternehmen zu infiltrieren, damit der Zugriff ausgeweitet werden kann und unternehmenskritische Daten und Systeme sowie Backups und Archive identifiziert werden können. Diese werden dann auf eine Attacke mittels verschiedener Angriffsarten vorbereitet.

Gerade vor dem Hintergrund, dass Cyberkriminelle den Unternehmen auch immer wieder einen Schritt voraus sind, ist es nicht verwunderlich, dass sich auch künftig im Rahmen von Künstlicher Intelligenz (KI) neue Möglichkeiten für Cyber-Angriffe anbieten und sich Cyberkriminelle diese zu nutzen machen. Alles, was KI positiv für Unternehmen zu tun vermag, kann auch zu Hacking-Zwecken genutzt werden. Einbeziehung von Logiken, Automatisierung und Deep Learning können auch für Hacker-Angriffe und das Ziel, an Daten oder in Unternehmensnetze zu gelangen, genutzt werden. Die Frequenz und Genauigkeit kann so deutlich steigen und die Bedrohungsszenarien müssen auf andere Art und Weise verteidigt werden.

Denkbar wäre in diesem Kontext, dass die Zahl von Botnetzen, wie jüngst das Mirai-Botnetz, die automatisiert und weitestgehend eigenständig Rechner befallen und als Ressourcen nutzen, sich noch rasanter vermehren. Zudem könnte eine „Hacking-KI" (z.B. AI-Generated Malware) zum Einsatz kommen, um politische Überwachungssysteme und die öffentliche Meinung durch Propaganda zu manipulieren. Denn fest steht, auch Hacker werden Künstliche Intelligenz nutzen. Durch „Hacking-KI" lassen sich weitere schwerwiegende Bedrohungsszenarien abbilden.

Der Weg an Daten zu kommen, wird durch den Einsatz von KI für Cyberkriminelle erheblich leichter. Jetzt sind Security-Anbietern und Unternehmen gefragt ebenbürtige Sicherheits-Technologien und Sicherheitsstrategien einzusetzen, um einem rasanten Anstieg von erfolgreichen Cyberangriffen entgegenzuwirken.

Security as a Service

Besonders durch den zunehmenden Vernetzungsgrad und die steigende Anzahl von kognitiven Systemen und die daraus resultierenden neuen Geschäftsprozesse verändert sich die Security-Landschaft innerhalb der Unternehmen sehr stark. Vor dem Hintergrund, dass diese Veränderungen auch neue Bedrohungsszenarien mit sich bringen, sind Führungskräfte gefragt die richtige IT-Security- und Datenschutz-Strategie zu definieren und zu exekutieren, den Einsatz von Security-Technologien zu nutzen, um Netze, Infrastrukturen und Daten zu schützen.

IT-Sicherheit und Datenschutz sollten demnach heute wie auch zukünftig als Querschnittsthema innerhalb der Unternehmen von innen nach außen gelebt werden – Daten sind von innen zu schützen – um den Pfad der Digitalisierung erfolgreich weitergehen zu können. Verschiedene Cloud-Angebote, insbesondere Cloud-basierte KI Security-Lösungen werden zunehmend wichtiger. Diese können die Anforderungen der neuen Security Dekade innerhalb der Unternehmen abdecken und zur Entscheidungsfindung bei der richtigen Security-Strategie mithelfen. Dabei stehen Datenschutz und IT-Sicherheit immer im Mittelpunkt. Auch von außen können Verordnungen, Maßnahmen und gesetzliche Entwürfe der Cyberkriminalität entgegenwirken.

Mit Security-as-a-Service (SECaaS) können Anforderungen an den Datenschutz, Compliance, Governance und IT-Sicherheit ganzheitlich gesteuert werden. So können Cyberattacken präventiv, detektiv und reaktiv behoben werden, zudem profitieren Unternehmen unter anderem durch:

- Aktuelle Versionen und regelmäßige Updates der Antivirenprogramme
- Schnellere Bereitstellung von Security-Lösungen
- Deutlich höhere Sicherheitsexpertise
- Regelmäßige Audits nach Compliance Vorgaben (BSI, Basel, SOX, usw.)
- Administration ausgewählter Bereiche, zum Beispiel Firewall-Regeln
- Individuelle Lösung/Strategie die auf bisherige Maßnahmen angepasst ist
- Machine Learning/ SaaS-AI Intrusion als 24/7 Service

Security by Design – der Schlüssel zur sicheren digitalen Transformation

Neben dem Schutz der Daten sollte aber auch die IT-Sicherheit, also der Schutz der Systeme, Netze und Infrastrukturen, in Einklang gebracht werden, um das Unternehmen auf neue Bedrohungsszenarien (z.B. Hacking-KI) einzustellen. Eine Möglichkeit IT-Sicherheit erfolgreich innerhalb der Unternehmen zu implementieren, ist das sogenannte Security by Design-Konzept. Im Rahmen der Studie **„Security by Design-Die Rolle von IT-Sicherheitsstrategien in der Digitalisierung"**, die Crisp Research in Kooperation mit der TÜViT veröffentlicht hat (*www.crisp-research.com/publication/security-design-die-rolle-von-it-sicherheitsstrategien-der-digitalisierung/*), werden die Möglichkeiten und der aktuelle Planungsstand dazu beleuchtet. Security-by-Design besagt, dass maßgeblich alle relevanten Maßnahmen im Kontext von Datenschutz und Sicherheit, schon von der Planungsphase einer neuen IT-Architektur beziehungsweise als DNA in der Produktentwicklung einbezogen werden sollten. Denn nur, wenn Unternehmen neue Wege gehen und Digitalisierung, Datenschutz, Sicherheit und den Faktor Mensch in der unternehmenseigenen Sicherheitsstrategie verei-

nen, kann es gelingen, gezielt und zügig einen organisatorischen Wandel einzuleiten und eine zentrale Sicherheitsstrategie zu schaffen.

Besonders vor dem Hintergrund neuen Bedrohungsszenarien werden die Charakteristika und Methoden der Security-Technologien zunehmend wichtiger. Mittels Lösungen aus dem Big Data/Analytics- und KI-Umfeld spielen Hacker und Unternehmen auf derselben Augenhöhe. Dies sollte auch als Weckruf an die Führungskräfte verstanden werden, existierende Sicherheits-Möglichkeiten rund um Big-Data und KI-Security konkret auszugestalten und in die eigene Sicherheitsstrategie mit einzubeziehen.

Hacker Tools und asymmetrische Kriegsführung

In den letzten 20 Jahren ist das Kompromittieren von Unternehmen zunehmend einfacher geworden. Im Netz erläutern diverse Anleitungen das Schreiben von Shellcodes und Exploits. Spezialliteratur, Hacker Tools und Videos auf Youtube erlauben es, selbst bei geringem Fachwissen in fremde Datenbanken einzudringen. Hinzu kommt, dass wir in einer nahezu vollvernetzten, verwobenen und digitalen Welt leben. Sogar Großunternehmen greifen auf Cloud-Dienstleistungen zurück, bieten Web 2.0 Anwendungen an und beschäftigen Dienstleister, die selber über das Internet auf ihre Daten zugreifen und diverse Teile ihrer IT outsourcen.

Das Paradigma des Verteidigers in der Burg wirkt damit schon lange nicht mehr. Dennoch halten viele Firmen an diesem alten und vermeintlich bewährten Konzept fest, ohne sich mit den realen Gegebenheiten und Gefahren der Gegenwart zu befassen. Angreifer und Verteidiger führen einen asymmetrischen Krieg. Während Unternehmen alle möglichen Sicherheitslücken und Schwachstellen identifizieren müssen, reicht dem Hacker nur ein einziges Schlupfloch, um verheerenden Schaden anzurichten. Das ökonomische Denken zeichnet den modernen Hacker aus, daher wählt er in der Regel folgendes Vorgehen:

- Mithilfe von automatisierten Hacker Tools wie Metasploit oder Nessus scannt er die IT-Landschaft des Ziels automatisch auf das Vorhandensein bekannter Sicherheitslücken. Findet der Hacker eine digitale Bruchstelle, schleust er sich ganz ohne fachliches Know-how ins System. Dann versucht er, sich auf weiteren Ebenen Zutritt zu verschaffen. Reichen Wissen und Können nicht, wird eine Hintertür installiert und der Zugang zu diesem System verkauft. Andernfalls weichen Hacker auf spätere Versuche aus.
- Führen automatisierte Hackerangriffe nicht zum gewünschten Erfolg, profitieren Hacker von der Faulheit des Menschen, einfache Passwörter komplizierten aber sicheren Kennungen den Vorzug zu geben. Schon zehn Rate-Versuche reichen

Schlupflöcher schließen

Hackerangriffe von morgen werden schon heute vorbereitet. Aus diesem Grund sollten Unternehmen mindestens folgende vier Maßnahmen umsetzen, um sich gegen einen Großteil der Hackerangriffe zu schützen:

1. Jede Schwachstelle mit einem CVSS (Common Vulnerability Scoring System)-Wert von 7 bis 9 muss innerhalb von 72 Stunden und jede mit einem Wert von 10 binnen 24 Stunden gepatcht werden. Drei der vier Maßnahmen, die laut dem Australia's Signals Directorate das Risiko einer gezielten Kompromittierung um 85 Prozent reduzieren, sind Patch-Maßnahmen.
2. Ein zentrales Log-Management mit spezifischen, auf die Bedürfnisse, Risiken und Anwendungszwecke angepassten Use-Cases ermöglicht eine adäquate Reaktion auf Kompromittierungsversuche, bevor tatsächliche Schäden eintreten.
3. Das Separieren von Netzwerken hilft bei der Reduktion von Netzwerkausfällen und erschwert das Ausbreiten von Malware oder Angreifern im Unternehmensnetzwerk.
4. Multi-Faktor-Authentifizierung (MFA) reduziert Hackerangriffe auf digitale Identitäten nahezu vollständig und stellen einen essentiellen Schutz für Mitarbeiter, Kunden und Lieferanten dar. Hacker müssten zwei unabhängig voneinander existierende Schranken passieren. Damit sollten nicht nur die internen Systeme, sondern auch dem Kunden angebotene Services wie Versicherungsportale oder SaaS-Anwendungen abgesichert werden.

Hackern, um 1 % der angegriffenen Accounts zu knacken. Bei einem Großunternehmen mit 10.000 Mitarbeitern sind das 100 Accounts, die Zugang zu sensiblen und wichtigen Daten haben. Haben Cyberganoven erst einmal die Barriere des Passwortes durchbrochen, kommen sie ohne weiteres an den meisten Sicherheitssystemen vorbei. Diese sehen keinen Handlungsbedarf, da der Account den Status „vertrauenswürdig" hat und das tut, wozu der berechtigt ist. Dem Erfolg der Hackerangriffe liegt die immer gleiche Ursache zugrunde: Eindimensionale, mehrfach benutzte, sich wiederholende Kennwörter und der Unwille, einen weiteren Faktor zu verwenden, öffnen dem Hacker sperrangelweit Tür und Tor. Laut dem Verizon 2017 Data Breach Investigations Report gehen 81 Prozent der Hackerangriffe auf gestohlene oder schwache Authentifizierungen zurück. Trotz der konstant bestehenden Gefahr verwenden User immer wieder dieselben simplen Wort- oder Zahlenkombinationen. „123456" etwa war im Jahr 2017 laut Hasso-Plattner-Institut Spitzenreiter unter den deutschen Passwörtern.

› Schlagen die ersten beiden Optionen fehl, greifen routinierte Hacker auf einen Mix aus Spear-Phishing, Social-Engineering oder physischen Maßnahmen zurück. Gute Spear-Phishing Mails, die auf perfekt gefälschte Webseiten führen, erkennen Laien auf den ersten Blick nicht. Neben dem Hauptziel, private Daten für räuberische Zwecke zu entwenden, spielt die Fake-Nachricht heimlich Malware auf den Rechner, die weiteren Schaden in Form von Computerviren anrichtet. Social-Engineering bildet eine der perfidesten Betrugsmethoden, da sie Emotionalität und Psyche des Menschen manipuliert. Hacker sammeln private Informationen aus verschiedenen Social-Media-Kanälen, um eine glaubwürdige fiktive Geschichte zu spinnen. Anschließend kontaktieren sie einen Mitarbeiter aus dem Unternehmen und schaffen durch einen Mix aus Fachjargon und Smalltalk über scheinbar gemeinsame Kollegen eine Vertrauensbasis. Führt das nicht zum Ziel, setzen sie Opfer durch Androhungen unter emotionalen Druck und nutzen menschliche „Schwachstellen" – Höflichkeit, Gutgläubigkeit oder die Unfähigkeit, Nein zu sagen. Insider kennen Geschichten, in denen sich Hacker als Techniker verkleidet Zugang zu Unternehmen verschafften oder sich als neue Mitarbeiter vorstellten und unschuldig nach dem Wifi-Passwort fragten. Das allein reicht schon aus, um sich im Netz einzunisten.

Bleiben alle drei Maßnahmen erfolglos, warten Hacker, bis eine neue Sicherheitslücke im System auftritt. Standardmäßig betragen die Patchzyklen in Unternehmen 30 bis 90 Tage – für eine sichere Hackerabwehr definitiv zu große Zeitabstände.

Fazit und Ausblick

Eines steht fest – die richtige Sicherheits-Strategie und Sicherheitslösungen aus dem Bereich der Künstlichen Intelligenz sind wichtiger denn je, gerade vor dem Hintergrund neuer Bedrohungsszenarien. Algorithmen und Machine Learning werden in diesem Kontext ein wichtiges Werkzeug, mit dem die Automatisierung noch einmal auf die nächste Stufe hebt, gerade hinsichtlich sicherheitsrelevanter Themen. Je besser Security-Analysen ausgewertet werden können und Datensets dieses Werkzeug durch Training verbessern, versprechen Künstliche Intelligenz beziehungsweise Machine Learning-Security Lösungen ein echter Game-Changer zu sein. Denn der hohe Vernetzungsgrad und der gleichzeitige Austausch von unternehmenskritischen Daten über das Internet Cyber-Kriminellen ein größeres Potential als je zuvor. Dies ist ein großes Problem, auf welches sich Unternehmen heute und auch zukünftig immer mehr einstellen müssen.

Jan Mentel und Dr. Amir Alsbih