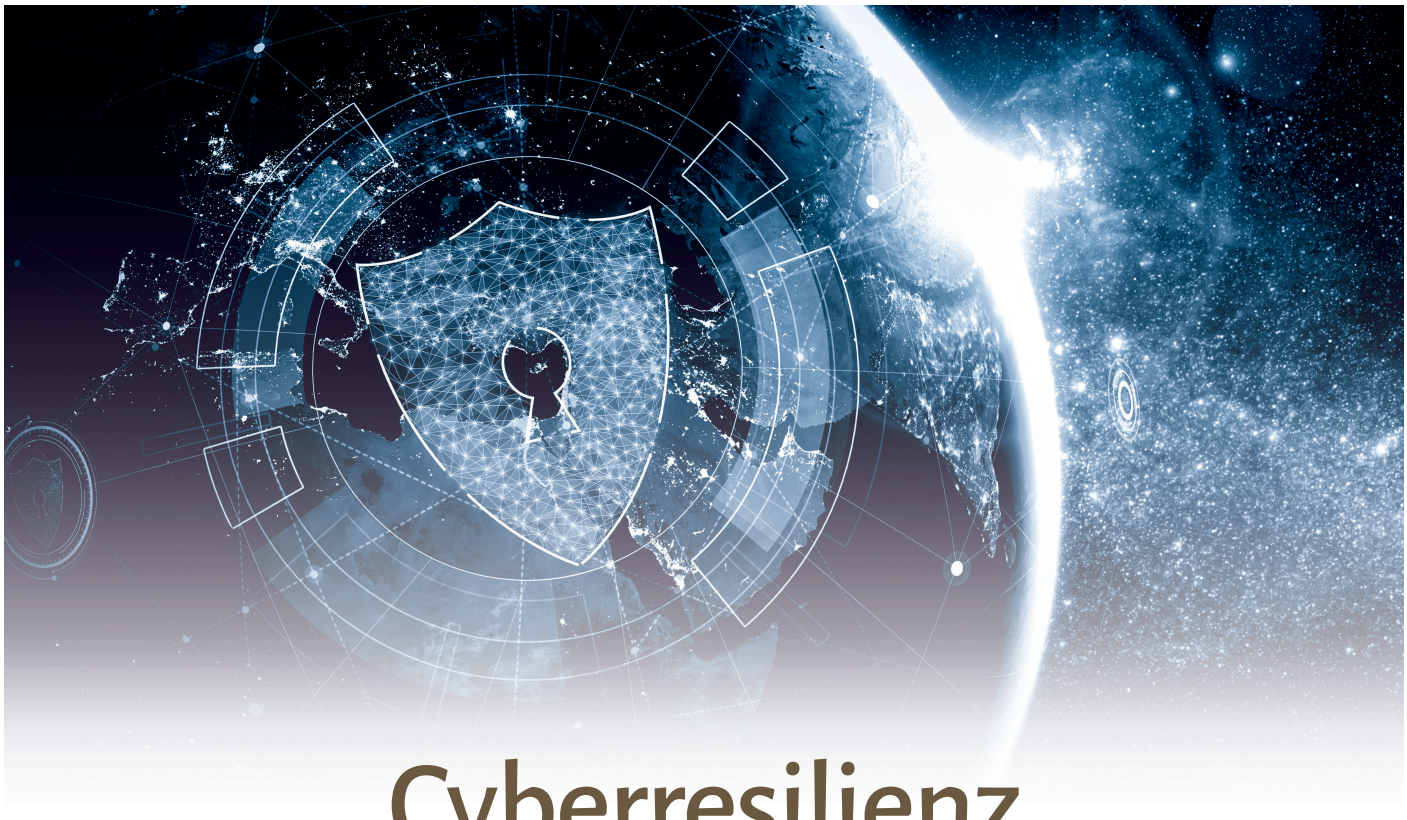

Cyberresilienz ist noch ein fernes Ziel

Sechs gängige Irrtümer hinsichtlich Cybersecurity im Unternehmen

Cybersecurity kostet Geld. Und solange IT-Systeme und Infrastruktur funktionieren, fällt es oft schwer, die nötigen Mittel zu investieren, um Risiken zu reduzieren und den reibungslosen Betrieb auch in Zukunft zu gewährleisten. Wenn aber Unternehmen ihr Cyberrisiko systematisch unterschätzen, hat dies mit verschiedenen Fehlannahmen zu tun.

Michael Niewöhner und Daniel Querzola

Sich mit Cybersecurity zu beschäftigen, ist eine eher ungeliebte Aufgabe. Dabei haben IT-Administrator:innen in vielen Fällen schon eine recht gute Vorstellung davon, woran es in ihrem Unternehmen hapert. Und wie die eigene IT prinzipiell auf den Prüfstand zu stellen wäre, damit Sicherheitslücken identifiziert und abgemildert oder gar ausgemerzt werden können. Dies heißt aber noch nicht, dass das Administrationsteam beim Management mit seinen Vorschlägen auch durchdringt. Woran das liegt, kann an sechs Irrtümern festgemacht werden:

Irrtum 1: Es trifft sowieso nur die anderen

„Unser Unternehmen ist für eine Cyberattacke doch gar nicht interessant genug." Diese Einschätzung ist alles andere als selten. Die Realität sieht leider vollkommen anders aus. Statistiken sprechen davon, dass sogar 99 Prozent aller Cyberschadensfälle auf Angriffe zurückgehen, die überhaupt nicht zielgerichtet waren. Anders formuliert: Die allermeisten Angriffe laufen nach dem Motto „Spray-and-Pray" ab.

Cyberkriminelle landen auch einen allgemeinen Angriffsversuch ohne konkretes Ziel. Dann warten sie einfach ab, bei welchen Unternehmen oder Organisationen beispielsweise die Mail mit dem Phishing-Link zum Erfolg führt. Leider ist bei vielen Unternehmen die Hürde für eine initiale Kompromittierung ihrer IT nicht hoch genug, um diesen Angriffen auf Dauer standzuhalten. Den Angreifern spielt dies in die Karten. Zumal dann, wenn sie vor allem finanzielle Interessen haben und das Unternehmen beispielsweise durch eine Verschlüsselung per Krypto-Trojaner bzw. »»

Ransomware erpressen wollen. Hier ist der Spray-and-Pray-Ansatz für Cyberkriminelle in der Regel am rentabelsten. Dies wiederum bedeutet: Jedes Unternehmen ist ein potenzielles Opfer.

Politisch motivierte Angriffe grenzen sich davon deutlich ab: Hier ist der Erfolg letztlich nur eine Frage der verfügbaren Arbeitskraft, denn bei einer ideologisch begründeten Attacke spielen monetäre Kosten-Nutzen-Abwägungen eine völlig nachrangige Rolle. In solchen Fällen kommen häufiger auch *Zero-Day-Angriffe* zum Einsatz, die noch nicht öffentlich bekannte Sicherheitslücken in einer Software ausnutzen. Mit einem Zero-Day-Exploit spielt der Angreifer gleichsam einen Joker aus. Denn wenn die neue Angriffsmethode durch ihren Einsatz publik wird, ist dieser Angriffsvektor letztlich verbrannt, weil Softwarehersteller dann entsprechende Sicherheitsupdates ausrollen.

Irrtum 2: Angriffe aus der Supply-Chain spielen keine Rolle

Tatsächlich nimmt die Zahl von Supply-Chain-Angriffen zu. Bei dieser Klasse von Cyberangriffen fungieren Softwarelösungen, Geräte oder Maschinen, die einem Unternehmen zugeliefert werden und die es für seine Geschäftstätigkeit einsetzt, als die Angriffsvektoren. So handelte es sich bei der *Log4j-Sicherheitslücke*, die im Dezember 2021 bekannt wurde, um eine Zero-Day-Schwachstelle in einer Java-Protokollierungsbibliothek. Log4j dient dazu, Protokollierungsinformationen aus Software, Anwendungen und Hardware-Appliances zu erstellen und zu speichern. Weil Log4j aber mitunter in vielen unterschiedlichen Lösungen sehr tief verankert ist, in tausenden Instanzen, reicht ein simpler Schwachstellenscan kaum aus, um hier alle angreifbaren Instanzen zu identifizieren.

Generell ist auch *Open-Source-Software* nicht vor Sicherheitslücken gefeit. So gelang es beispielsweise einem Professor der University of Minnesota im Kontext einer Studie, Schwachstellen in den Linux Kernel einzuschleusen. Dazu gaben er und einer seiner Studenten vor, Bug Fixes für die Linux Community bereitzustellen. Ziel der umstrittenen Aktion war es, zu demonstrieren, wie angreifbar auch Open-Source-Projekte sein können. Eine Sicherheitslücke im Linux Kernel ist potenziell so gravierend, weil Linux sehr weit verbreitet ist. Es findet sich heute in Servern und Smartphones und auch in verschiedenen Embedded Devices.

Mit der zunehmenden Digitalisierung von Wirtschaft und Lebenswelt können heute eben auch vernetzte Geräte zum Einfallstor für Cyberkriminelle werden. So wurde etwa eine Supermarktkette gehackt, indem die Angreifer die intelligenten Kühlregale in den Geschäften als Angriffsvektor wählten. Für vernetzte Geräte im Smart-Home-Bereich besteht dasselbe Risiko. Auch sie stellen potenzielle Angriffspunkte dar – ein gravierendes Reputationsrisiko für den Gerätehersteller oder -vertreiber.

Im privaten wie im kommerziellen Raum ist darum ein viel bewussterer Umgang mit installierter Software und angeschafften Geräten erforderlich. Im produzierenden Gewerbe beispielsweise, wo eine Maschine einen Lebenszyklus von mehreren Jahrzehnten haben kann, stehen früher oder später meist nur noch mildernde Maßnahmen zur Verfügung, um Sicherheitsrisiken zu reduzieren. Denn Hersteller existieren dann nicht mehr, oder sie liefern nach wenigen Jahren keine Sicherheitspatches mehr. So bleibt mitunter als einzige Option noch, die Maschine aufwendig vom restlichen Netzwerk abzuschotten und das Restrisiko zu akzeptieren.

Grundsätzlich gilt: Es wäre für ein Unternehmen fahrlässig, wollte es die Verantwortung für seine Cybersicherheit gänzlich auf die Zulieferer abwälzen. Bedrohungen aus der Supply Chain heraus sind real und heute alltäglich. Unternehmen benötigen deshalb nicht nur ein entsprechendes Risikobewusstsein, sondern auch Experten und Expertinnen, die sie dabei unterstützen, eine effektive Cyberresilienz zu etablieren.

Irrtum 3: Mitarbeiter:innen haben genügend Sicherheitsbewusstsein

Noch viel zu oft stellt ein unbedachtes Verhalten der Mitarbeiter:innen für Cyberkriminelle ein bequemes Einfallstor ins Unternehmen dar. Ein entsprechendes Risikobewusstsein zu schaffen und wachzuhalten, ist ein Baustein für Cybersicherheit, dessen Bedeutung ein Unternehmen nie unterschätzen sollte. Nur wenn ihnen die Gefahr bewusst ist, werden es die Beschäftigten konsequent vermeiden, beispielsweise Passwörter über das Telefon weiterzugeben oder unbedacht auf einen dubiosen Link in einer E-Mail zu klicken. Manchmal ist das Gefahrenpotenzial auch eine unmittelbare Konsequenz der täglichen Arbeit. Mitarbeiter:innen in der Personalabteilung etwa öffnen beinahe täglich Bewerbungen, ohne wissen zu können, ob der digitale Lebenslauf Schadcode enthält oder nicht. Mit Rechnungs-PDFs im Maileingang der Buchhaltung verhält es sich genauso. Darum braucht es im Unternehmen natürlich technische Maßnahmen gegen solche Angriffe.

Aber ebenso wichtig ist es, die Wahrscheinlichkeit erfolgreicher Phishing-Versuche zu verringern, indem ein Bewusstsein für die Gefahren von *Social-Engineering-Angriffen* ganz allgemein geschaffen wird. Social Engineering bedeutet, dass die Angreifenden Täuschung anwenden, um unautorisiert Daten oder Zugriff zu bekommen. Dabei werden Methoden der Humanpsychologie dazu missbraucht, Mitarbeiterr:innen zu manipulieren und sie zur Übermittlung von Informationen oder zu bestimmten Handlungen zu bewegen – wie etwa den fatalen Klick auf den Link in der Phishing-E-Mail oder die Nennung des Passworts gegenüber vermeintlichen Support-Mitarbeitenden am Telefon.

Irrtum 4: Die Sicherheitsprüfung wird schon ausreichen

Die Cybersicherheit im Unternehmen durch *Penetration Tests* auf die Probe zu stellen, ist ein wichtiger Baustein im Aufbau der Cyberresilienz. Wählt man dabei allerdings den Scope des *Pentests* zu klein, ist wenig gewonnen. Denn so entsteht ein vermeintliches Gefühl von Sicherheit. Ein typisches Beispiel ist der Ausschluss bestimmter Systeme, etwa solcher, die am Ende ihres Lebenszyklus stehen, weil sie ja sowieso bald abgeschaltet oder ersetzt werden. Solange sie noch nicht abgeschaltet sind, bieten aber gerade diese Altsysteme oft den verführerischsten Angriffsvektor.

Wenn Pentests wirklich aussagefähig werden sollen, dürfen sie sich nicht nur auf einen Ausschnitt der Unternehmens-IT richten. Vielmehr müssen sie holistisch angelegt sein. Denn das Ziel eines Penetration-Tests ist es nicht, dem Management ein positives Gefühl in Sachen Cybersicherheit zu vermitteln – er soll wirkliche Sicherheitslücken und potenzielle Angriffsvektoren identifizieren.

Irrtum 5: Pentests kann die IT nebenher übernehmen

Penetration-Tests können in den meisten Unternehmen gar keine Inhouse-Aufgabe sein. Denn IT-Administratoren und -Administratorinnen haben vor allem eines zu tun: Sie müssen dafür sorgen, dass die Systeme im Unternehmen zuverlässig laufen. In der Regel ist das Administrationsteam mit seinen operativen Aufgaben bereits zu 100, wenn nicht gar zu 120 Prozent ausgelastet. Zudem verlangen Penetration-Tests ein hochspezialisiertes und hochaktuelles Fachwissen, über das die eigene IT-Abteilung in der Regel gar nicht verfügen kann.

Gleichzeitig muss den Mitarbeiter:rinnen der internen IT klar sein, dass es bei einer Sicherheitsprüfung nie darum geht, ihre eigene Arbeit in Sachen Cybersecurity zu diskreditieren, sondern zu stärken. Ein aussagefähiger Penetration-Test wäre mit Inhouse-Ressourcen gar nicht durchführbar, weil Know-how und Zeit dafür fehlen.

Irrtum 6: Unsere Backups retten uns im Notfall

Vor etwas mehr als fünf Jahren mag diese Aussage vielleicht noch zutreffend gewesen sein. Heute ist sie das nicht mehr, nicht in jedem Fall. Man muss sich vor Augen führen, dass die Qualität von Schadsoftware deutlich gestiegen ist. *Krypto-Trojaner*, die Unternehmensdaten zu Erpressungszwecken verschlüsseln, tun dies heute nicht mehr unverzüglich. Es gibt inzwischen Ransomware, die sich zuerst in den Backups eines Unternehmens einnistet und diese nach und nach zerstört. Erst Monate später, wenn das Backup unbrauchbar geworden ist, macht sich der Krypto-Trojaner dann daran, die Daten des Unternehmens zu verschlüsseln – und die eigentliche Erpressung beginnt. Darum ist es heute wichtig, Backups erstens mit geeigneten Schutzkonzepten vor Malware zu sichern und sie zweitens regelmäßig zu prüfen. Nur auf ein Backup, das auch tatsächlich aufsetzbar ist, ist im Notfall Verlass. Unternehmen sollten darum ihre *Disaster Recovery* regelmäßig testen, üben und ausprobieren. Und wenn ein Unternehmen sein Backup aus Sicherheitsgründen verschlüsselt: Auch dieser Backup-Schlüssel selbst ist ein möglicher Angriffspunkt, denn Cyberkriminelle können natürlich auch den Backup-Schlüssel des Unternehmens verschlüsseln. Das Backup wäre dann wiederum unbrauchbar, und der Erpressungsversuch durch die Verschlüsselung der Unternehmensdaten könnte beginnen. Darum ist es wichtig, dass Unternehmen ihre Krypto-Schlüssel für das Backup offline aufbewahren und auch ihr Notfalltraining in Sachen Disaster Recovery offline dokumentieren.

Fazit: Die Gefahr von Cyberangriffen hat nicht abgenommen, im Gegenteil. Wollte ein Unternehmen aus einer glimpflich verlaufenen Vergangenheit schließen, dass es auch in Zukunft vor Cyberkriminalität sicher ist, wäre dies vielleicht die gravierendste Fehlannahme von allen. Operative Zuverlässigkeit lässt sich in der IT nur herstellen, wenn ein Unternehmen seine Cyberresilienz mit geeigneten, holistischen Konzepten und Maßnahmen etabliert, aufrechterhält und weiterentwickelt. Sich damit auseinanderzusetzen, lohnt die Mühe in jedem Fall, denn der finanzielle Schaden wiegt im Ernstfall um ein Vielfaches schwerer. Auch in Sachen Cybersecurity gilt: Vorbeugen ist besser als heilen. ■

INFORMATION & SERVICE

AUTOREN

Michael Niewöhner ist bei Ventum Consulting als Manager für IT Security & Penetration Testing tätig. Niewöhner ist Offensive Certified Security Professional.

Daniel Querzola ist bei Ventum Consulting als Manager IT Security & Penetration Testing tätig. Zu seiner Kernexpertise gehört es, Audits im Kontext komplexer Unternehmensarchitekturen durchzuführen.

KONTAKT

Ventum Consulting GmbH & Co. KG
Kontakt: info@ventum.de