HEFT 1-2 | JANUAR-FEBRUAR 2025 | 23. JAHRGANG SONDERDRUCK

manage it

IT-STRATEGIEN UND LÖSUNGEN

KI, Cybersicherheit, Cloud und vieles mehr

IT-TRENDS 2025

Wo bleibt der ROI bei KI?

Pragmatischer Ansatz

Unterdigitalisiert und überreguliert

Digitalstrategie sorgt für ein Win-Win-Verhältnis

Datenmanagement

Innovationen brauchen Datenstrategie

SPEZIAL SECURITY

ab Seite 59

Cyberangriff – was nun?

Wie Unternehmen gezielt reagieren und vorbeugen

Früher oder später trifft es jedes Unternehmen. Wie können sie Angriffe erkennen, im Ernstfall angemessen reagieren und sich besser davor schützen? Ein kurzer Leitfaden für die IT-Sicherheit in Zeiten von »Cybercrime-as-a-Service«.

Eines vorweg: Deutsche Unternehmen machen vieles richtig. Bei ihren Bemühungen um die Cybersecurity bekommen interne und externe Fachkräfte zudem Unterstützung vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dessen Angebot von Basisinformationen zum IT-Grundschutz über Themen wie Cloud Computing bis hin zur kostenlosen Mitgliedschaft in der Allianz für Cybersicherheit reicht.

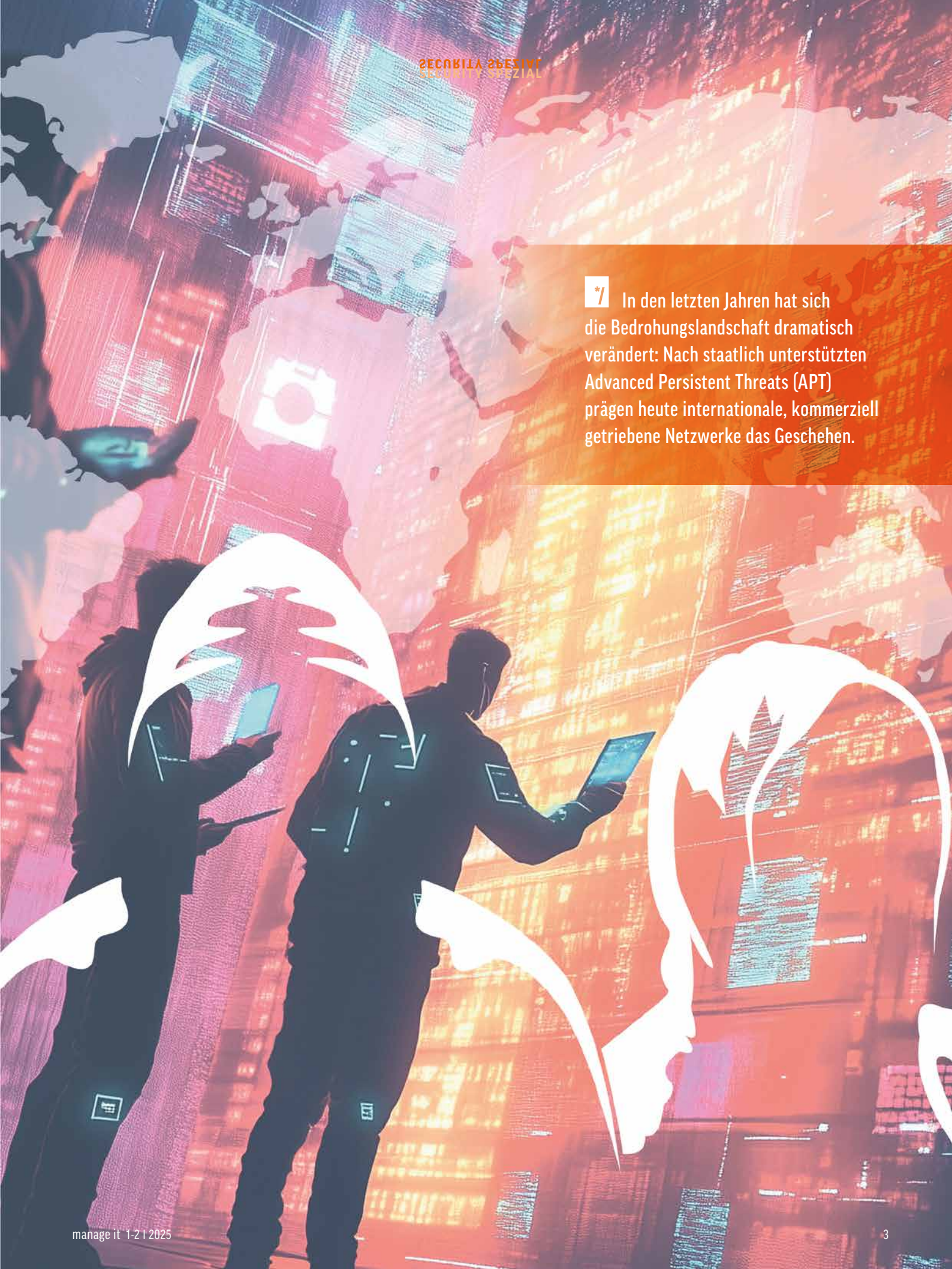
Und doch stellt sich auch bei vorbildlicher Praxis nicht die Frage, ob das Unternehmensnetzwerk durch einen Cyberangriff kompromittiert wird, sondern wann. Klar ist auch, dass es sich kein Unternehmen leisten kann, erst im Ernstfall darüber nachzudenken, was vor, während und nach einem Vorfall zu tun ist.

Arbeitsteilung bei den Angreifern. In den letzten Jahren hat sich die Bedrohungslandschaft dramatisch verändert: Nach staatlich unterstützten Advanced Persistent Threats (APT) prägen heute internationale, kommerziell getriebene Netzwerke das Geschehen. Nach Angaben des Bundeskriminalamtes haben die Auslandstaten im Jahr 2023 im Vergleich zum Vorjahr um rund 28 Prozent zugenommen. Kriminelle Dienstleistungen werden mittlerweile im industriellen Maßstab nach dem Geschäftsmodell »Cybercrime as a Service« angeboten. Hochspezialisierte Banden teilen sich die Aufgaben vom operativen Geschäft über das Management bis hin zum Overhead.

Die vorherrschende Angriffsart der kommerziellen Cybercrime-Szene ist Ransomware. Nach einer bundesweiten Auswertung des BKA und der Landeskriminalämter haben im vergangenen Jahr mehr als 800 Unternehmen und Institutionen entsprechende Fälle gemeldet, wobei von einer hohen Dunkelziffer auszugehen ist. Bei einem Ransomware-Angriff verschaffen sich Angreifer zunächst Zugang zum Unternehmensnetzwerk. Sie sehen sich um, entwenden Daten und verschleiern ihre Spuren durch Verschlüsselung. Ziel ist es, die Opfer arbeitsunfähig zu machen und zu erpressen, oft sogar doppelt: erst durch Verschlüsselung und dann mit der Drohung, die gestohlenen Daten zu veröffentlichen. Weit verbreitet ist auch die Bedrohung durch Business E-Mail Compromise (BEC). Bei dieser Methode, vor der kürzlich die Cybercrime-Stelle Nordrhein-Westfalen warnte, schleichen sich Angreifer in die E-Mail-Daten und -Kommunikation von Mitarbeitenden ein, um finanzielle Transaktionen zu manipulieren.

Wo setzen die Angreifer an? Die initiale Kompromittierung erfolgt in der Regel über den Menschen: Mittels Phishing versuchen die Angreifer, ihre Opfer zur Preisgabe von Zugangsdaten zu bewegen, indem sie sich in der Unternehmenshierarchie immer weiter nach oben arbeiten. Aus technischer Sicht sind Firewalls und VPN-Gateways die wichtigsten Einfallstore, die über das Internet erreichbar, aber nicht ausreichend geschützt sind. Zum Beispiel, weil der Zugang nicht durch eine Multi-Faktor-Authentifizierung (MFA) gesichert, oder die Software nicht aktuell ist. Eine weitere potenzielle Schwachstelle sind persönliche Webzugänge zu Cloud-Diensten wie Microsoft 365. Sind diese nicht ausreichend gesichert, gelingt es Angreifern häufig, sich über den Browser als »Organisation« anzumelden und Zugriff auf Unternehmensdaten zu erhalten.

Viele Unternehmen bemerken einen Cyberangriff daher erst, wenn es bereits zu spät ist oder kurz davor. Ursachen sind unter anderem unzureichende Sicherheitsvorkehrungen oder fehlende Frühwarnsysteme, so dass Anomalien in der Systemlandschaft nicht rechtzeitig erkannt werden. Nicht selten wird der Angriff erst entdeckt, wenn einige



In den letzten Jahren hat sich die Bedrohungslandschaft dramatisch verändert: Nach staatlich unterstützten Advanced Persistent Threats (APT) prägen heute internationale, kommerziell getriebene Netzwerke das Geschehen.

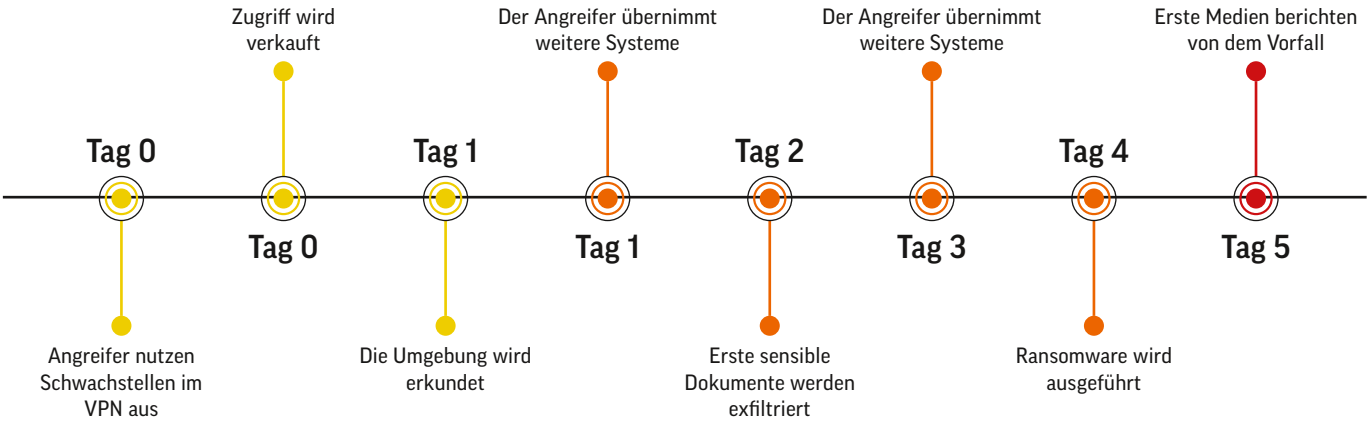


Abbildung 1: Schon wenige Tage nach der Attacke übernehmen Angreifer das System.

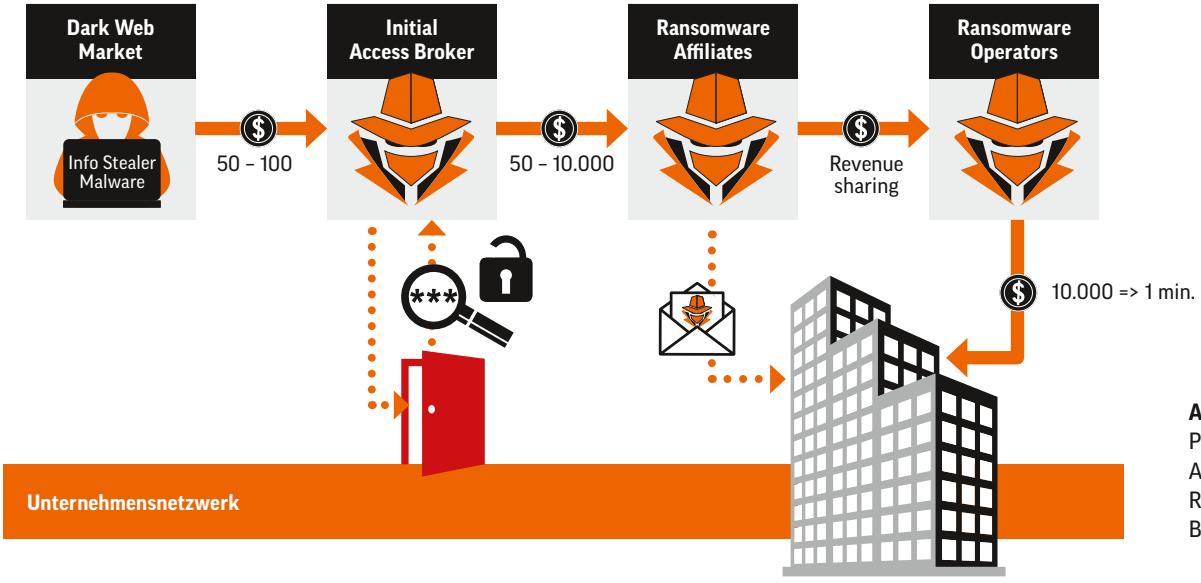


Abbildung 2: Professionelle Arbeitsteilung von Ransomware-Banden.

Prozesse oder Apps nicht mehr funktionieren oder wenn Warnmeldungen von Sicherheitsanbietern überprüft werden.

To-Dos bei einem Cyberangriff. So schlimm es auf den ersten Blick auch aussehen mag, lautet die goldene Regel dennoch: Ruhe bewahren, selbst bei Verschlüsselung. Denn wer im Ernstfall überstürzt handelt und die Server abschaltet, verschlimmert die Situation unter Umständen nur, da wertvolle Beweise vernichtet werden. Zudem ist das kriminelle Ziel in der Regel bereits erreicht, wenn der Angriff bekannt wird. So vergeht etwa bei finanziell motivierten Angriffen immer etwas Zeit, bis der nächste Teilschritt erfolgt. Initial Access Broker »verkaufen« beispielsweise ihr Projekt nach erfolgreichem Zugriff an einen Ransomware-as-a-Service-Anbieter, der Datenexfiltration und Systemverschlüsselung übernimmt.

Wie Unternehmen und Dienstleister richtig auf einen Cyberangriff reagieren, hängt daher vom jeweiligen Szenario ab. In einem ersten Schritt ist es ratsam, herauszufinden, welche Daten gestohlen wurden und als wie kritisch diese zu bewerten sind. Bei sensiblen Informationen wie personenbezogenen Daten oder unternehmenskritischen Patenten sollte sofort die »Notbremse« gezogen werden, um den Schaden zu begrenzen. Dies ist auch der Fall, wenn der Angreifer die Privilegien eines Domain-Administrators erlangt hat oder wenn VIPs wie die Geschäftsführung oder andere wichtige Personen betroffen sind.

Kein direkter Handlungsbedarf besteht hingegen, wenn lediglich eine Hintertür eingebaut wurde, aber keine Verhaltensänderung festzustellen ist. In diesem Fall ist die Backdoor zu schließen und der Vorfall umfassend zu analysieren. Ähnlich verhält es sich, wenn das Netzwerk nur kleinflächig und abgrenzbar mit Schadcode infiziert ist oder nur unkritische Daten abgeflossen sind.

Da es keinen absoluten Schutz vor Cyberangriffen gibt, ist das wirksamste Instrument für den Ernstfall ein sofort

umsetzbarer Notfallplan. Dieser im Vorfeld zu entwickelnde Handlungsleitfaden legt Krisenstäbe und Maßnahmen fest, so dass klar ist, wer wofür zuständig ist und wie gezielt auf verschiedene Bedrohungsszenarien reagiert werden soll. Infolge einer gründlichen Risikoabschätzung wird auch festgelegt, welche Daten, Informationen und Server unbedingt geschützt werden müssen und welche kriminellen Handlungen im Ernstfall noch toleriert werden.

Präventionsmaßnahmen. Nach jedem Vorfall ist es wichtig, die Ereignisse gründlich aufzuarbeiten, also zu analysieren, welche Maßnahmen erfolgreich waren und wo Verbesserungspotenzial besteht. Eine gründliche Nachbereitung hilft, künftigen Angriffen besser vorzubeugen und die Widerstandsfähigkeit des Unternehmens zu stärken. Wertvolle Erkenntnisse sollten in die Cyberstrategie und den Notfallplan einfließen.

Ein optimaler Schutz gegen Angriffe beginnt mit der genauen Kenntnis über die eigene Systemlandschaft. Denn nur so lassen sich auch ohne Tools eigene Prozesse, Applikationen und Services von kriminellen unterscheiden. Wer EDR (Endpoint Detection and Response) oder weiterführende Response-Lösungen einsetzt, sollte auf eine hohe Erkennungsquote achten. Ein konsequentes Patch- und Update-Management sowie regelmäßige Backups an einem Speicherort außerhalb des Unternehmensnetzwerks sind ebenfalls unerlässlich.

Trotz aller eigener Maßnahmen fehlt es meistens an der erforderlichen Expertise und den personellen Ressourcen. Besser geeignet ist daher ein ganzheitlicher Managed-Detection-and-Response-Ansatz (MDR), der nicht nur Schutzmaßnahmen wie EDR, sondern auch Incident Response, Compromise Assessments oder Data Breach Assessments umfasst.

Während Incident Response eine schnelle Reaktion auf ungeplante Ereignisse oder Dienstunterbrechungen ermöglicht, spüren Compromise Assessments laufende Angriffe und Malware auf. Data Breach Assessments wiederum forschen im Darkweb nach Hinweisen auf noch unentdeckte Angriffe. Werden diese Maßnahmen im Rahmen eines MDR-Ansatzes miteinander verzahnt, können Angriffe frühzeitig erkannt und effektiv abgewehrt werden. Das Fazit lautet also: Es ist entscheidender, welche Sicherheitsmaßnahmen man vor einem Angriff etabliert, anstatt hinterher bloß zu reagieren.

Yasin Ilgar,
Managing Cyber Defense Consultant,
SECUINFRA GmbH

https://www.secuinfra.com/de/