heise Business Services

Ein eBook von

Powered by T-Systems

Hacking 2.0

Angriffs- und Verteidigungsstrategien in einer komplexen IT-Welt

Extra

Expertenmeinung

Wie reduziere ich Geschäftsausfälle durch unvorhergesehene Betriebsunterbrechungen?

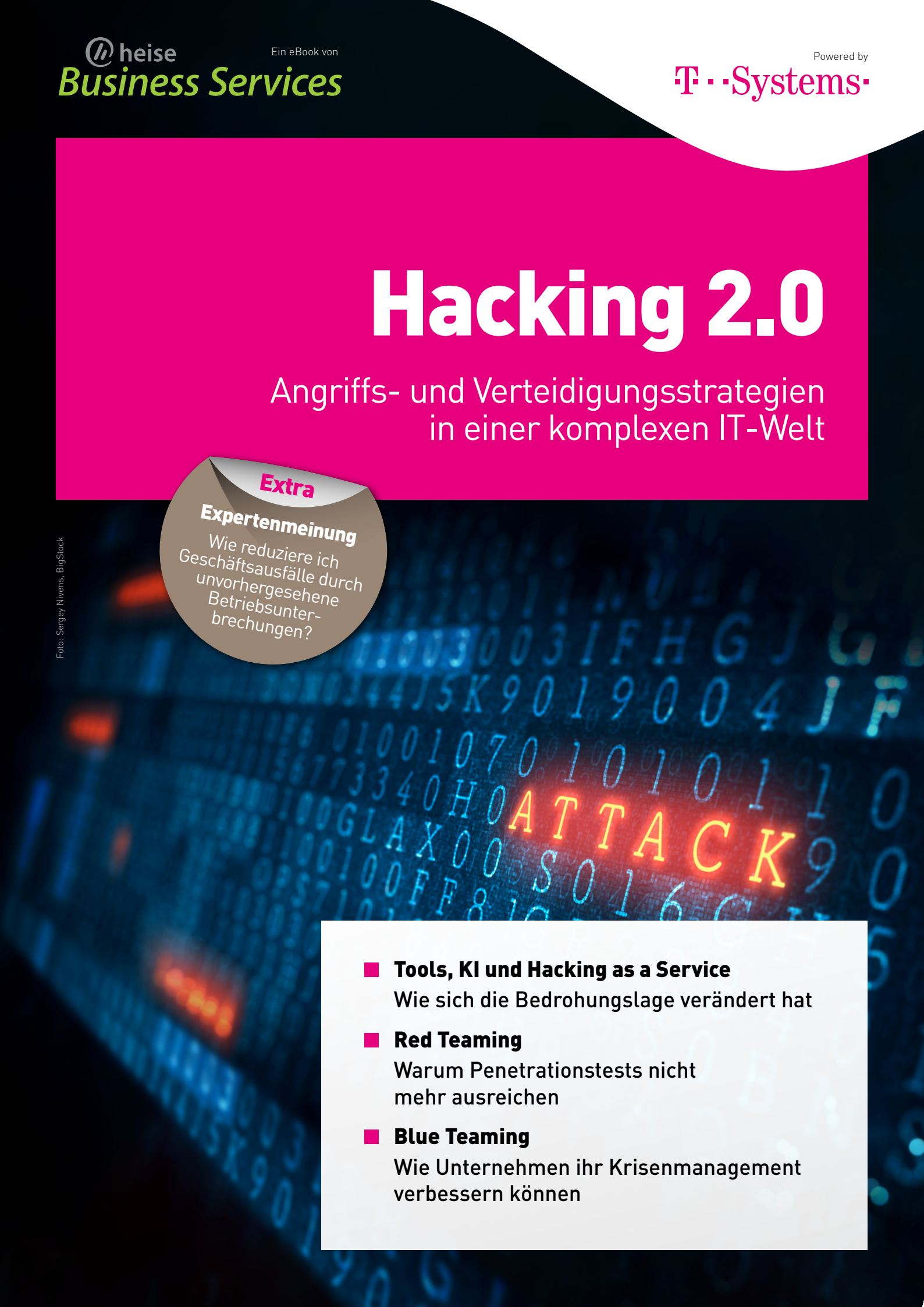


Foto: Sergey Nivens, BigStock

- **Tools, KI und Hacking as a Service**
  Wie sich die Bedrohungslage verändert hat
- **Red Teaming**
  Warum Penetrationstests nicht mehr ausreichen
- **Blue Teaming**
  Wie Unternehmen ihr Krisenmanagement verbessern können

Foto: Sergey Nivens, BigStock

Editorial

Cyberkriminelle haben es heute leichter denn je. Viren und Trojaner lassen sich einfach aus Malware-Baukästen zusammenbauen, Hacking-Dienstleistungen „as a Service“ aus dem Darknet beziehen. Auch das organisierte Verbrechen hat diese Chance längst erkannt und Cyberkriminalität zum lukrativen Geschäftsmodell entwickelt. Von langer Hand geplante und professionell durchgeführte Angriffe sind deshalb keine Seltenheit mehr.

Unternehmen tun daher gut daran, ihre Abwehrmaßnahmen zu verstärken und sie in regelmäßigen Abständen auf ihre Wirksamkeit zu prüfen. Traditionelle Penetrationstests genügen dafür allerdings nicht mehr. Sie konzentrieren sich zu sehr auf die technischen Aspekte der Verwundbarkeit und berücksichtigen den Faktor Mensch nicht. Unbedachtes oder falsches Verhalten von Mitarbeitern ist aber ein mindestens ebenso großes IT-Sicherheitsrisiko wie Software-Schwachstellen oder offene Ports. Erfolgreiche Social-Engineering-Attacken, etwa über Phishing-Mails, überwinden mit Leichtigkeit die besten technischen Abwehrmaßnahmen.

In den vergangenen Jahren wurde daher das Red-Team-/Blue-Team-Konzept immer beliebter, mit dem sich der Sicherheitsstatus einer Unternehmens-IT ganzheitlich prüfen, evaluieren und verbessern lässt. Dabei treten Sicherheitsexperten in zwei Teams aus Sicherheitsexperten als Angreifer (Red Team) und Verteidiger (Blue Team) gegeneinander an. Allerdings hat auch dieser Ansatz Optimierungspotenzial. So ist es unter Umständen effizienter, wenn Red und Blue Team in einem „Purple Team“ zusammenarbeiten. Mehr dazu erfahren Sie in diesem eBook.

Dr. Thomas Hafen
Freier Journalist

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de

Inhalt

ÜBER DEN AUTOR

Dr. Thomas Hafen war über 15 Jahre als Redakteur, Moderator und Manager für verschiedene IT-Fachverlage tätig. Seine fachlichen Schwerpunkte liegen in den Bereichen Digitale Transformation, Cloud Computing und Advanced Analytics. Thomas Hafen lebt und arbeitet heute als freier Journalist und Moderator in München.

Foto: smolaw, BigStock

Tools, KI und Hacking as a Service

Wie sich die Bedrohungslage verändert hat

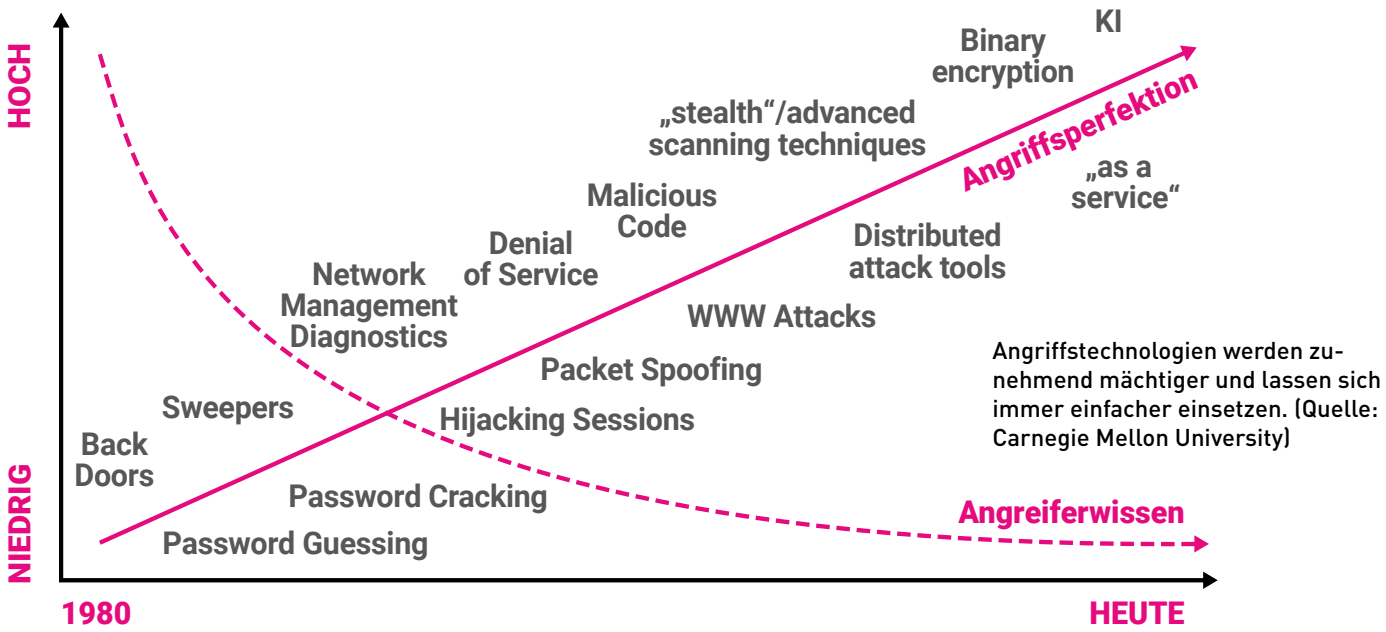
Hacking ist längst nicht mehr nur eine Freizeitbeschäftigung für frustrierte Teenager, sondern zu einer milliardenschweren Industrie geworden. Das hat Konsequenzen für die Verteidigungsstrategien der Unternehmen.

Wannacry, Petya und Emotet: In den vergangenen Jahren haben es Cyber-Angriffe immer häufiger in die Schlagzeilen geschafft. Betroffen waren unter anderem prominente Opfer wie die Deutsche Bahn, der Industriekonzern KraussMaffei oder die Heise Gruppe. Allein für das Jahr 2018 vermeldet das Bundeslagebild Cybercrime des Bundeskriminalamtes (BKA) fast 90.000 Fälle mit einem Schaden von über 60 Millionen Euro. Weltweit sind die Zahlen noch bedenklicher: Die von Accenture und dem Pokemon Institute herausgegebene Studie „The Cost of Cybercrime" vermeldet für 2018 durchschnittlich 145 Sicherheitsvorfälle pro Unternehmen, elf Prozent mehr als 2017 und 67 Prozent mehr als fünf Jahre zuvor. Die durchschnittlichen jährlichen Cybercrime-Gesamtkosten pro Unternehmen stiegen gegenüber 2017 von 11,7 Millionen auf 13 Millionen US-Dollar, im Fünfjahresvergleich betrug die Steigerung 72 Prozent.

Konsumerisierung der Cyberkrimimalität

Diese Zunahme sowohl der Zahl als auch der Schwere der Attacken hat verschiedene Gründe: Wie in vielen anderen Bereichen der IT ist auch in der Cyber-Kriminalität eine „Konsumerisierung" zu beobachten: Angriffswerkzeuge und -services werden immer mächtiger und gleichzeitig immer einfacher zu bedienen. Es ist kein großes Fachwissen mehr nötig, um IT-Systeme anzugreifen. Ransomware und Hacking-Dienste lassen sich „as a Service" aus dem Internet beziehen. Skripte und Rootkits stehen teilweise offen in Foren zum Download zur Verfügung und werden vor allem von Jugendlichen – sogenannten Script Kiddies – eingesetzt. Sicherheitsforscher wie das MalwareHunterTeam oder Misterch0 stellen seit Längerem fest, dass diese Möchtegern-Hacker immer jünger werden. Auch wenn die Angriffe wenig ausgefeilt sind und sich die Malware-Verteiler oft selbst infizieren, können sie doch erheblichen Schaden verursachen. Einem Blog-Beitrag der Sicherheitsfirma Checkpoint zufolge konnte beispielsweise ein einzelner 20-Jähriger mit einfachsten Hacking-Tools über vier Monate hinweg mehr als 4.000 Unternehmen auf der ganzen Welt angreifen. Zu den Opfern gehörten Banken, Energieversorger, Minenbetreiber und Baufirmen.

> Wie in vielen anderen Bereichen der IT ist auch in der Cyber-Kriminalität eine „Konsumerisierung"zu beobachten.



Angriffstechnologien werden zunehmend mächtiger und lassen sich immer einfacher einsetzen. (Quelle: Carnegie Mellon University)

In der organisierten Kriminalität herrscht zudem mittlerweile eine sehr starke Arbeitsteilung. Spezialisierte Teams kümmern sich um die Suche von Schwachstellen in Produkten, andere entwickeln Angriffswerkzeuge, wieder andere planen Attacken und führen sie durch. Hinzu kommen flankierende Services wie Geldwäsche und andere Dienstleistungen. Diesen Trend bestätigt eine erst kürzlich erschienene Studie, die sich mit sozialen Strukturen in der organisierten Cyber-Kriminalität beschäftigt (E. R. Leukfeldt, Thomas J. Holt: Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline, International Journal of Offender Therapy and Comparative Criminology 2019). Den Autoren zufolge sind diese Organisationen heute hauptsächlich in Teams und formellen unternehmensähnlichen Hierarchien strukturiert. Allein bei Phishing-Attacken identifizierten die Autoren Netzwerke mit bis zu vier Ebenen und bis zu neun verschiedenen Rollen und Aufgabengebieten (Koordinatoren, Anrufer, Kassierer, Bank- und Postangestellte, Entwickler für Phishing-Webseiten, Passfälscher, Geldkuriere und deren Anwerber). Den Schaden, den die organisierte Internetkriminalität anrichtet, beziffern Leukfeldt und Holt unter Bezug auf diverse Untersuchungen auf einen Betrag zwischen 445 Milliarden und 600 Milliarden US-Dollar pro Jahr.

Künstliche Intelligenz im Dienst der Cyber-Kriminalität

Künstliche Intelligenz (KI) spielt auch in der IT-Security eine immer größere Rolle. Kaum eine Sicherheitslösung kommt heute noch ohne KI-Komponente aus. Algorithmen kommen zum Einsatz, um Muster und Anomalien in großen Datenmengen zu entdecken, die Identifikation von Phishing-Mails und Malware zu verbessern oder um verdächtiges Kommunikationsverhalten etwa in Bot-Netzen zu erkennen. Analysten schätzen, dass der globale Markt für KI-basierte Security-Lösungen bis 2025 auf 24 Milliarden US-Dollar ansteigen wird.

Aber auch die Gegenseite rüstet mit KI auf. Mithilfe von Machine Learning lassen sich beispielsweise anhand weniger Minuten Ausgangsmaterial Sprachprofile erstellen und damit täuschend echte Audiobotschaften beliebigen Inhalts generieren. Auch wenn dieser Trick nicht neu ist und in den USA schon seit einigen Jahren verwendet wird, erhält die KI-basierte Stimmenimitation doch immer größere Bedeutung, vor allem im Bereich des Geschäftsführerbetrugs, auch „CEO-Fraud" oder „Whaling" genannt. Dabei meldet sich ein hochrangiger Manager, der gerade auf Auslandreise ist, in der Finanzbuchhaltung und verlangt die sofortige Überweisung großer Geldsummen, um ein wichtiges Geschäft abschließen zu können. Häufig geben die attackierten Buchhalter unter dem hohen Zeitdruck, den der Anrufer aufbaut, und dessen massiven Drohungen nach und überweisen die geforderte Summe, ohne sich vorher rückzuversichern. Erst wenn das Geld längst in dunklen Kanälen verschwunden ist, stellt sich heraus, dass der Anruf gefälscht war.

Ein weiterer Bereich, in dem KI in Zukunft eine große Rolle spielen könnte, ist das sogenannte Spear Phishing, also die gezielte Ansprache einer Person mit auf sie zugeschnittenen E-Mails oder Chat-Nachrichten. Intelligente Bots können soziale Netze, Foren und Firmenseiten sehr viel schneller und effizienter nach Informationen durchforsten, Zusammenhänge herstellen und Schwachstellen identifizieren als menschliche Angreifer. Auch die Formulierung optimal auf die Zielperson abgestimmter E-Mails, Facebook-Nachrichten oder Tweets kann man der KI überlassen. Einmal eingedrungen, finden trainierte neuronale Netze dank Mustererkennung und semantischer Analyse zuverlässig sensible Daten und schleusen sie geschickt aus dem Unternehmensnetzwerk, ohne verhaltensbasierte Überwachungsmechanismen auszulösen.

Fazit

Konsumerisierung, Arbeitsteilung, KI – IT-Sicherheitsverantwortliche müssen sich auf immer mehr und immer raffiniertere Angriffe einstellen. Vor allem die Zahl gezielter Attacken ist signifikant gestiegen. Aber auch wer glaubt, er sei zu klein oder zu unbedeutend für einen Angriff, sollte sich nicht zu sicher fühlen. Denn auch die Zahl automatisierter Attacken steigt, die spezifische Schwachstellen ausloten oder mit immer besseren Phishing-Mails arbeiten. Unternehmen haben darüber hinaus mit der zunehmenden Komplexität ihrer IT-Umgebung zu kämpfen. Cloud, IoT und Mobile Computing haben die Angriffsfläche massiv ausgeweitet, der klassische Perimeterschutz ist als alleiniger Verteidigungswall gegen Angriffe nicht mehr ausreichend. Angesichts der aktuellen Bedrohungslage benötigen Unternehmen daher neue Strategien, um Angriffe abzuwehren oder zumindest erfolgreiche Attacken schneller zu entdecken. ■

> Künstliche Intelligenz (KI) spielt auch in der IT-Security eine immer größere Rolle.

Foto: megaflopp, BigStock

Red Teaming

Warum Penetrationstests nicht mehr ausreichen

Beim Red-Team-Ansatz, auch Ethical Hacking genannt, betrachten Security-Experten die IT-Infrastruktur aus dem Blickwinkel eines Angreifers. Das ermöglicht einen ganzheitlichen Blick auf das Sicherheitsniveau eines Unternehmens.

Unternehmen fällt es immer schwerer, erfolgreiche Angriffe zu entdecken und so schnell wie möglich einzudämmen. Laut dem von IBM herausgegebenen „Cost of a Data Breach Report 2019" benötigten Betroffene 206 Tage, um einen Datendiebstahl zu erkennen, und weitere 73 Tage, um ihn einzudämmen – ein Anstieg von fast fünf Prozent gegenüber dem Vorjahr. Klassische Abwehrmaßnahmen wie Vulnerability Scans und Penetrationstests reichen offensichtlich nicht aus, um Angriffe abzuwehren oder zumindest erfolgreiche Attacken schnell zu entdecken. Sie fokussieren sich typischerweise auf technische Angriffs- und Abwehrszenarien und prüfen nur einzelne Aspekte der IT-Infrastruktur, etwa die Verwundbarkeit der Server, des Webshops oder mobiler Zugänge. Der Komplexität moderner IT-Umgebungen werden sie damit allerdings nicht mehr gerecht. Es besteht zudem die Gefahr, dass bei „Brute-Force"-Penetrationstests sehr viel Zeit und Aufwand in Angriffe auf gut gehärtete Strukturen gesteckt wird, während die Einfallstore in benachbarten Bereichen liegen. Auch der menschliche Faktor wird bei rein technischen Penetrationstests außer Acht gelassen. Viele erfolgreiche Angriffe sind auf menschliches Fehlverhalten zurückzuführen. Awareness-

> Klassische Abwehrmaßnahmen reichen offensichtlich nicht aus, um Angriffe abzuwehren.

Schulungen und Sicherheitstrainings können daran nur bedingt etwas ändern, da Menschen unter Druck dazu neigen, reflexartig zu handeln, statt ruhig zu bleiben, kontrolliert zu handeln und erlerntes Wissen anzuwenden.

Der Red- und Blue-Team-Ansatz

In der IT-Sicherheit kommt daher immer häufiger ein Konzept zum Einsatz, das aus militärischen Übungen bekannt ist. Es werden zwei Teams – „Red" und „Blue" – gebildet, die gegeneinander antreten. Das rote Team hat die Aufgabe, die Sicherheitsvorkehrungen zu überwinden, das blaue muss sie verteidigen. Nach dem „Capture the Flag"-Ansatz wird meist ein konkretes Ziel vereinbart, welches das Rote Team erreichen muss. Es muss also beispielsweise in ein bestimmtes System eindringen oder eine bestimmte Datei stehlen können. Im Unterschied zu klassischen Penetrationstests beschränkt sich das Rote Team nicht auf die separate Anwendung einzelner technischer Methoden, sondern kombiniert die verschiedensten Angriffsvektoren, um zum Ziel

zu kommen. Dazu gehören auch Maßnahmen wie Social Engineering und Phishing. Natürlich sind dabei rechtliche Vorgaben zu beachten und etwa der Betriebsrat mit einzubeziehen.

Wann sich Red Teaming lohnt

Der Red-Team-Ansatz bietet sich immer dann an, wenn es nicht um die Härtung einzelner Systeme und Umgebungen wie eines Webshops, einer Cloud-Lösung oder eines Systems von Überwachungskameras geht, sondern das gesamte Sicherheitsniveau des Unternehmens betrachtet werden soll. Er bietet eine umfassende Sicht auf mögliche Risiken und kann bereits erfolgte Einbrüche leichter nachvollziehbar machen. Insgesamt kann ein Red-Team-Assessment vor allem Antworten auf folgende Fragen geben:

- **Greifen meine Sicherheitsvorkehrungen wie geplant?**
- **Wie gut bin ich tatsächlich gegen Angriffe gewappnet?**
- **Kenne ich alle potenziellen Schwachpunkte und Einfallstore?**

Pentesting vs. Red Teaming

Im Vergleich zu Pentests analysieren Red-Team-Assessments komplette Systemumgebungen. (Quelle: TechTarget)

Penetration-Testing	Red Teaming
Zeitraum für das Testen ist kurz.	Zeitraum für das Testen ist erweitert.
Tester nutzen kommerzielle Pen-Test-Tools.	Das Team wird zu kreativem Denken angeregt und motiviert, alles Verfügbare zum Testen zu verwenden.
Mitarbeiter bemerken, dass getestet wird.	Mitarbeiter bemerken in der Regel nicht, dass getestet wird.
Tester versuchen, bekannte Schwachstellen auszunutzen.	Tester versuchen neue Schwachstellen zu entdecken.
Testziele sind vordefiniert.	Testziele sind veränderlich und durchlaufen mehrere Bereiche.
Systeme werden unabhängig voneinander getestet.	Systeme werden parallel getestet.

Die Phasen eines Red-Team-Assessments

Red-Team-Assessments unterscheiden sich in mehreren Punkten von klassischen Penetrationstests: Sie finden meist über einen längeren Zeitraum statt und werden nicht angekündigt. Während in Pentests hauptsächlich kommerziell erhältliche Tools zum Einsatz kommen, die nach bekannten Schwachstellen suchen, ist beim Red Teaming Kreativität gefragt, um neue Angriffspunkte und Einfallstore zu finden. Pentests analysieren zudem ein System nach dem anderen, während im Red-Team-Assessment simultan die gesamte IT-Umgebung betrachtet wird.

Ein Red-Team-Assessment läuft in der Regel in folgenden Phasen ab:

- **Taktische Informationsbeschaffung:** Das rote Team analysiert, über welche Wege das vorgegebene Ziel erreicht werden könnte. Welche Mitarbeiter spielen eine Schlüsselrolle? Wo ließe sich ein präparierter USB-Stick am besten platzieren? Welche Systeme weisen bekannte Lücken auf? Gibt es offene Ports oder nur mit Standardpasswörtern gesicherte Zugänge?

- **Vorbereitung:** Auf Basis der gewonnenen Informationen entwirft das rote Team eine Strategie, identifiziert geeignete Ziele und schreibt Angriffsskripte.

- **Angriff:** Das rote Team beginnt mit seiner Attacke. Zunächst wird versucht, Systeme direkt aus dem Internet zu kompromittieren, um sich eine bessere Position für weitere Angriffe zu verschaffen. Als Nächstes versucht das rote Team, Mitarbeiter per Social Engineering zum Download und zur Ausführung infizierter Dateien zu bringen, indem es gezielt Malware per E-Mail, Chat-Nachricht oder Tweet an sie adressiert oder ihnen USB-Sticks mit Schadcode zusendet. Unter Umständen versucht das rote Team auch, physischen Zugang zu den IT-Systemen zu erlangen, um sie direkt zu manipulieren.

- **Lateral Movement:** Einmal eingedrungen gilt es, sich höhere Privilegien und Zugang zu geschäftskritischen Systemen zu verschaffen.

- **Exfiltration und Sabotage:** Ist das rote Team am eigentlichen Ziel angekommen, stiehlt es Daten oder legt Systeme lahm, ohne dass Warnsysteme wie DLP (Data Loss Prevention) Alarm schlagen.

- **Verstecken und Beobachten:** Mit Remote-Access-Trojanern, die Audio- und Videodaten übertragen können, behält das rote Team die Aktivitäten im Unternehmen im Blick.

- **Abschluss und Dokumentation:** Nach erfolgreicher Mission oder nach Ablauf der vereinbarten Zeit informiert das rote Team die Unternehmensführung über den Ausgang des Assessments, erklärt sein Vorgehen und gibt Hinweise für Verbesserungsmaßnahmen.

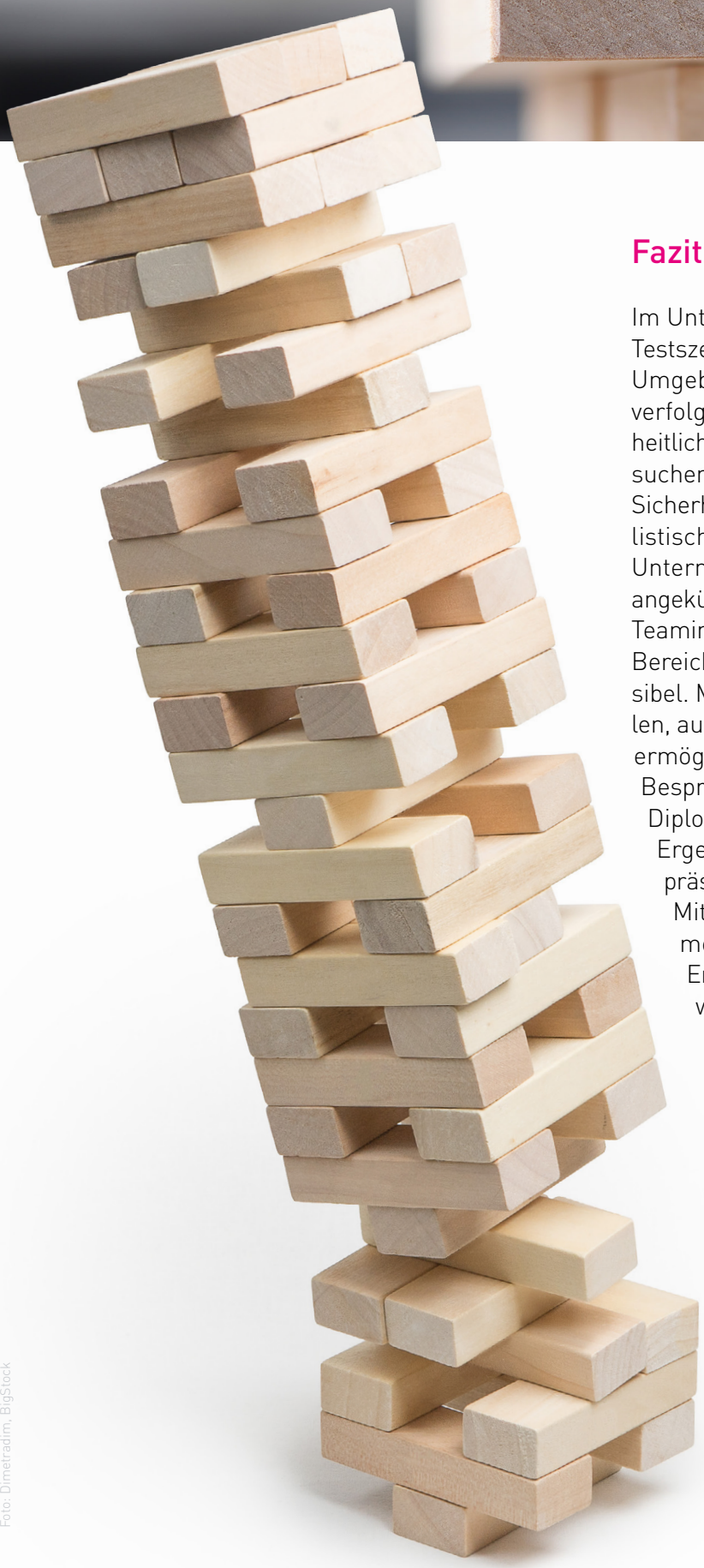


Foto: Dimetradim, BigStock

Fazit

Im Unterschied zu Penetrationstests und anderen Testszenarien, die isoliert bestimmte Systeme oder Umgebungen auf Schwachstellen untersuchen, verfolgt das Red-Team-Assessment einen ganzheitlicheren Ansatz. Die Mitglieder des roten Teams suchen gezielt nach dem schwächsten Glied in der Sicherheitskette und ermöglichen so einen viel realistischeren Blick auf das Sicherheitsniveau eines Unternehmens, als es mit isolierten und vorab angekündigten Testszenarien möglich ist. Das Red Teaming birgt jedoch auch Risiken. Besonders der Bereich menschlichen Fehlverhaltens ist sehr sensibel. Mitarbeiter dürfen sich nicht bloßgestellt fühlen, auch wenn sie das Eindringen des Red Teams ermöglicht haben. Sowohl die Angriffe als auch die Besprechung der Ergebnisse sind deshalb mit viel Diplomatie und Feingefühl durchzuführen und Ergebnisse gegebenenfalls nur anonymisiert zu präsentieren. Es darf nicht darum gehen, einzelne Mitarbeiter bloßzustellen. Das Ziel muss vielmehr sein, aus den Fehlern zu lernen, die zum Erfolg des Red Teams geführt haben, und notwendige Verhaltensänderungen so zu verankern, dass sie auch in Stress- und Ausnahmesituationen abgerufen werden können. ■

Foto: PramoteBigstock BigStock

Blue Teaming

Wie Unternehmen ihr Krisenmanagement verbessern können

Angesichts hybrider, komplexer Infrastrukturen und immer raffinierterer Angriffsmöglichkeiten scheint die Verteidigung einer IT-Infrastruktur gegen Eindringlinge durch das Blue Team nahezu unmöglich. Aber auch für den Fall, dass das Team scheitert, lassen sich aus den Erfahrungen wertvolle Hinweise auf das Krisenmanagement eines Unternehmens gewinnen.

In den vergangenen Jahren haben nicht nur die Cyber-Kriminellen aufgerüstet, auch die Unternehmen haben massiv in eine bessere Verteidigung ihrer IT-Umgebungen investiert. Allein im Jahr 2019 stiegen nach Berechnungen des Analystenhauses IDC die weltweiten Ausgaben für Security-Lösungen um fast zehn Prozent gegenüber dem Vorjahr. Sie liegen nunmehr bei rund 103 Milliarden US-Dollar. Der Markt wird laut IDC auch in den kommenden Jahren in diesem Tempo weiterwachsen. In Europa ist Deutschland nach Großbritannien der zweitgrößte Abnehmer von Cybersecurity-Lösungen und -Services. Rund 20 Prozent der europäischen Investitionen in IT-Sicherheit entfallen auf deutsche Unternehmen, Behörden und andere Organisationen.

> Panische Reaktionen auf eine erfolgreiche Attacke können mehr Schaden anrichten als der Angriff selbst.

Häufig führt diese technische Aufrüstung jedoch nicht zum gewünschten Erfolg. Lösungen wie SIEM (Security Information and Event Management), IDS / IPS (Intrusion Detection / Prevention System), EDR (Endpoint Detection and Response) und andere liefern zwar eine Fülle von Log-Informationen, doch in vielen Fällen verwirrt die Datenmenge eher, als sie hilft. Einer Umfrage von Osterman Research zufolge ist beispielsweise ein Drittel der SIEM-Nutzer von der Leistung der Systeme enttäuscht. Der Anteil von Fehlalarmen (False Positives), den diese Systeme auslösen, kann bis zu 70 Prozent betragen. Die Bedienung ist zudem sehr personalaufwendig. Osterman rechnet mit mindestens zwei Vollzeitstellen für das Management.

In vielen Fällen fehlt es aber nicht nur an den Personalressourcen, sondern auch an den notwendigen Kenntnissen, um diese Daten wirklich auswerten, die richtigen Schlüsse daraus ziehen und geeignete Gegenmaßnahmen einleiten zu können. Es existieren zudem keine Krisenpläne – niemand weiß, was im Notfall konkret zu tun ist. Oft richten panische Reaktionen auf eine erfolgreiche Attacke sogar mehr Schaden an als der Angriff selbst.

Das Blue Team und seine Bedeutung für die Sicherheitslage

Im Red-Team- / Blue-Team-Ansatz hat das Blue Team die Aufgabe, den Gegner (= das Red Team) aufzuspüren und ihn daran zu hindern, in Systeme oder vordefinierte Ziele einzubrechen. Dafür hat es auf den ersten Blick sehr schlechte Karten. Eine 100-prozentige Verteidigung von IT-Systemen ist nicht realistisch. Die Grenzen der IT-Infrastruktur eines Unternehmens sind oft undefiniert und ändern sich ständig, während es die Komplexität erschwert, den Überblick zu behalten, Anwendungen sind nur schwer auf dem neuesten Stand zu halten. Unachtsamkeit und Fehler der Mitarbeiter öffnen den Angreifern Tür und Tor. Darüber hinaus sind die Organisationen ständig mit der Gefahr von Zero-Day-Exploits konfrontiert, die einen gegnerischen Zugriff ermöglichen. Hinzu kommt das Problem der Schatten-IT. Rechner, Smartphones oder sogar WLAN-Router und andere Netzwerkgeräte werden an der IT-Abteilung vorbei ins Firmennetz gebracht, Cloud-Dienste und Chat-Apps genutzt, ohne auf deren Compliance zu achten. Nicht umsonst vergleicht Chris Dale vom SANS Institute die Aufgabe des Blue Teams mit der eines Torwarts, dessen Torpfosten sich ständig verändern und der mit unterschiedlichsten Bällen beschossen wird.

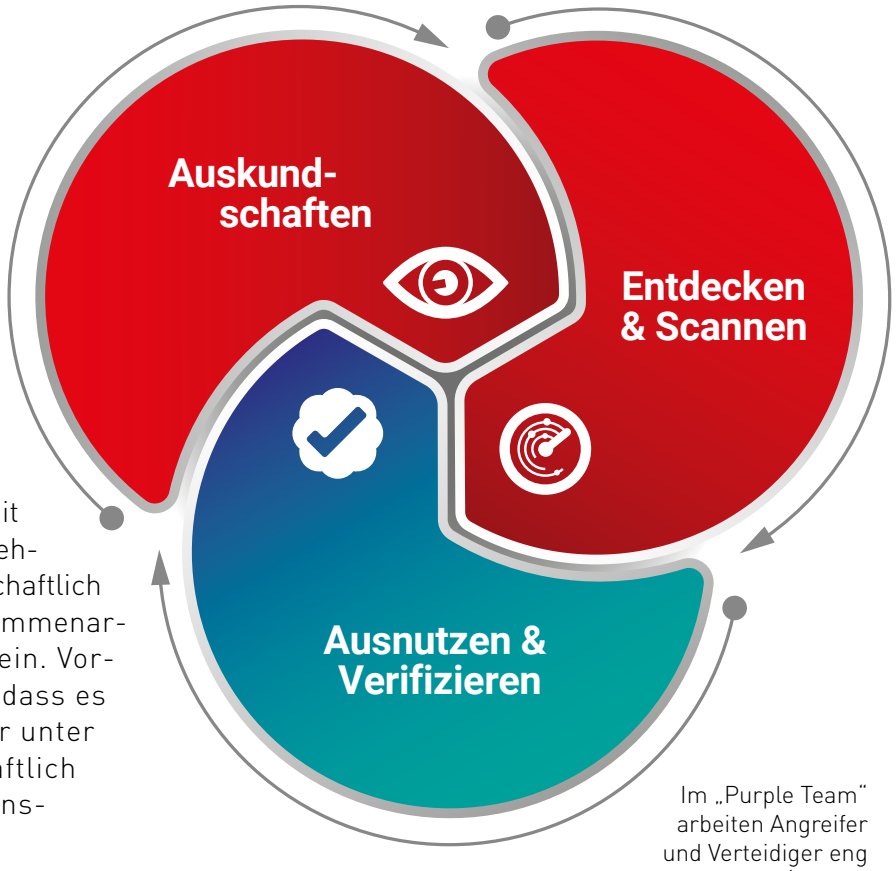
Das programmierte Scheitern sollte jedoch nicht zu Frust und Enttäuschung beim Blue Team führen. Aus dem Erfolg des Red Teams lassen sich nämlich viele wichtige Erkenntnisse über das Sicherheitsniveau eines Unternehmens gewinnen. Wer sich verteidigen will, muss schließlich wissen, wie man angreift. Es findet daher ein Wissenstransfer über das Vorgehen der Angreifer und die Verteidigungsmöglichkeiten statt. Wie reagiert das Blue Team auf einen erfolgreichen Angriff? Wie nützlich sind die Gegenmaßnahmen? Was muss verändert und verbessert werden? Diese und ähnliche Fragen lassen sich nach solchen Angriffsmanövern zuverlässiger beantworten. Gerade Krisensituationen müssen zudem immer und immer wieder durchgespielt werden. Nicht umsonst führen Feuerwehr und Rettungskräfte regelmäßige Übungen durch, in denen sie Einsätze unter realistischen Bedingungen proben.

Wenn Red und Blue Team verschmelzen

Der Red-Team- / Blue-Team-Ansatz ist allerdings in jüngster Zeit auch in die Kritik geraten. SANS-Experte Chris Dale hält ihn beispielsweise für überholt. Er schlägt dagegen die Bildung eines „Purple Teams“ vor, in dem beide Seiten zusammenarbeiten. So könnte etwa das Red Team sehr viel Zeit und Energie sparen, wenn es nach einer ersten Schwachstellenanalyse seine Ergebnisse mit dem Blue Team teilt, statt lange und vergeblich jede nur erdenkliche potenzielle Sicherheitslücke durchzutesten. Dieser Ansatz ist wesentlich kostengünstiger als beispielsweise ein vollständiger Penetrationstest. Er führt außerdem dazu, dass die verschiedenen Teams Vertrauen zueinander aufbauen können. Gemeinsam erarbeiten die Teams dann einen Maßnahmenplan und identifizieren möglicherweise bislang noch nicht entdeckte Sicherheitslücken. Häufig kommt das Red Team auch schnell und einfach über leicht zu erratende Anmeldedaten oder bekannte Schwachstellen zum Ziel, während das Blue Team mit viel Aufwand an anderer Stelle Systeme härtet und Sicherheitsmechanismen implementiert. Auch hier bewahrt der schnelle Informationsaustausch vor Fehlinvestitionen, Zeitverlust und unnötigen Risiken.

Fazit

Der Red-Team- / Blue-Team-Ansatz ist eine erprobte und häufig verwendete Methode, das Sicherheitsniveau eines Unternehmens zu analysieren, Schwachstellen zu identifizieren und Maßnahmen für deren Behebung zu definieren. Eine Zusammenarbeit beider Teams in einem Purple Team kann helfen, Zeit und Kosten zu sparen und schneller zu einem Ergebnis zu kommen. Der Erfolg eines solchen Assessments steht und fällt allerdings immer mit einer geeigneten Fehlerkultur im Unternehmen. Nur wenn alle Beteiligten partnerschaftlich und ohne Angst vor Gesichtsverlust zusammenarbeiten, wird dieser Ansatz erfolgreich sein. Vorgesetzte sollten klar kommunizieren, dass es nicht darum geht, einzelne Mitarbeiter unter Druck zu setzen, sondern gemeinschaftlich an der Verbesserung der Unternehmenssicherheit zu arbeiten. ■



Im „Purple Team" arbeiten Angreifer und Verteidiger eng zusammen. (Quelle: SANS Institute)

”

Beim Purple-Team-Ansatz bewahrt der schnelle Informationsaustausch vor Fehlinvestitionen, Zeitverlust und unnötigen Risiken.

Expertenmeinung

Wie reduziere ich Geschäftsausfälle durch unvorhergesehene Betriebsunterbrechungen?

T · · Systems · Let's power higher performance

Was Sie über Cyber-Attacken wissen sollten

Die 10 wichtigsten Geschäfts-risiken in Deutschland

Cyber-Attacken in deutschen Unternehmen

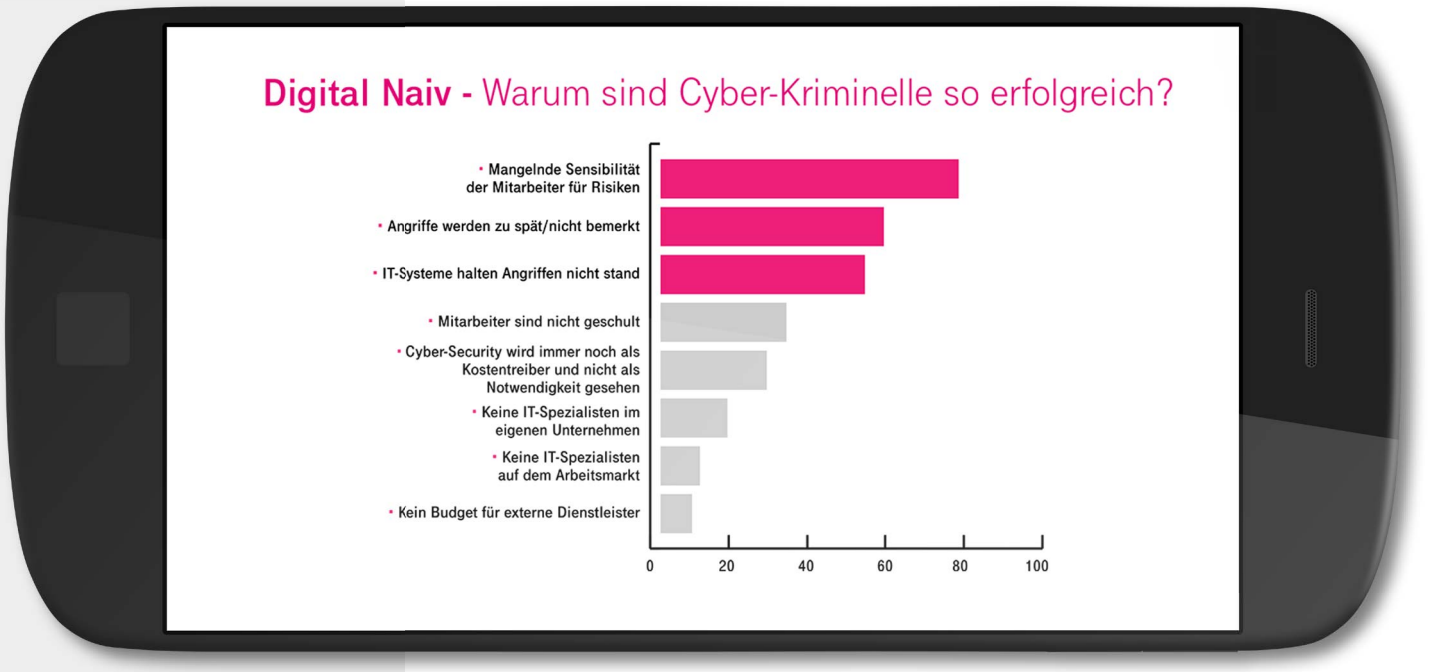
Die geschäftskritischen Vorfälle in deutschen Unternehmen steigen kontinuierlich, wie die nachfolgende Grafik verdeutlicht. Cyber-Vorfälle finden sich unter den wichtigsten zehn Geschäftsrisiken in Deutschland mittlerweile auf Platz 2; in der globalen Einschätzung sind IT-Ausfälle, Cyberkriminalität, Datenschutzverletzungen und damit einhergehende Geldbußen und Strafen sogar Risiko Nummer 1. Das hohe Tempo der Digitalisierung und des technologischen Wandels schafft ständig neue Angriffspunkte der Businessstabilität und umso stärker (und häufiger) wird Notfall- und Krisenmanagement (Emergency and Crisis Management) zu Cyber Crisis Management.

Quelle:
Allianz Global Corporate & Specialty, Allianz Risk Barometer 2020

Cyber-Attacken – ein Hauptgrund für Betriebsunterbrechungen

Zukünftige Schwachstellen in Unternehmen

Jede Minute werden über 4.000 Datensätze gestohlen.[1] Die von der Deutschen Telekom ausgelegten Honeypots - also Köder für Hacker– registrierten im April 2020 bis zu 46 Millionen Hackerattacken an einem Tag – Tendenz steigend.[1] Teilweise werden die Angriffe“ „as a Service“ angeboten und identisch professionell angeboten und vermarktet wie im realen Markt. Mit hoher Wahrscheinlichkeit wird der Angriff über Ransomware die häufigste Ursache sein, womit sich die IT Abteilungen beschäftigen müssen. Seit Jahren steigen die Angriffe und der damit verbundene Schaden für Unternehmen.



Quelle:
Wirtschaftswoche 2019,
„Der nette Angreifer“

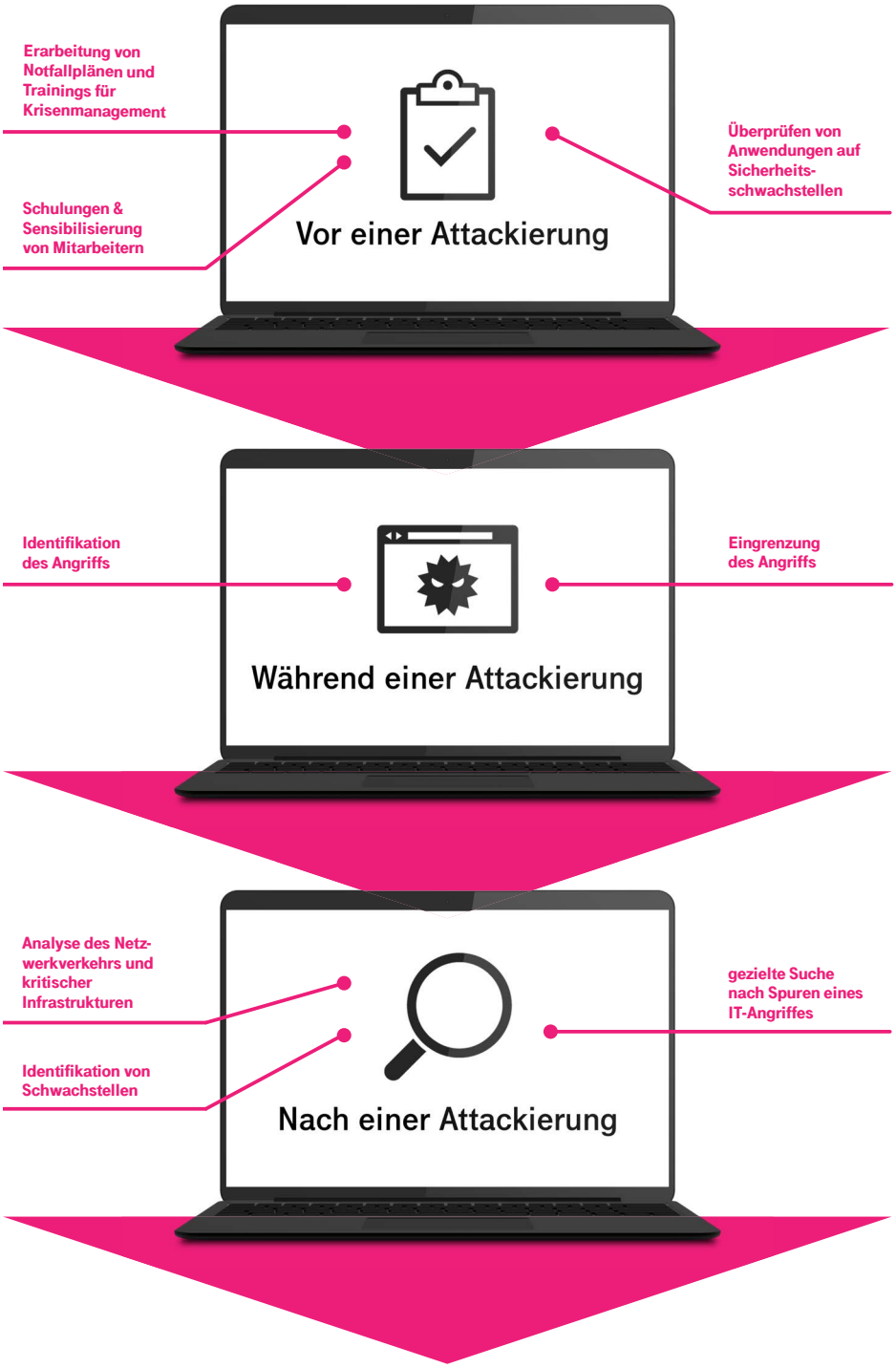
Leider gibt es keine hundertprozentige Sicherheit vor Cyber-Angriffen, egal wie gut man versucht, sich zu schützen. Insbesondere der Faktor „Mensch“ ist und bleibt unberechenbar und die größte Schwachstelle. Dennoch kann man mit guter Vorsorge und einer ganzheitlichen Strategie Risiken minimieren und die möglichen Ausfallzeiten reduzieren.

1: Deutsche Telekom Security GmbH
https://www.sicherheitstacho.eu/start/main

Was Sie über Cyber-Attacken wissen sollten

Mit ganzheitlicher Strategie Risiken vermeiden

Bei der Auswahl sollten immer 3 Szenarien berücksichtigt werden: was kann ich im Vorfeld tun, um mich bestmöglich zu schützen? Wie reagiere ich während eines Angriffs? Und welche Möglichkeiten stehen mir nach einem Angriff zur Verfügung, um möglichst schnell wieder einsatzfähig zu sein und für die Zukunft zu lernen?



Expertenmeinung

Wie gehe ich mit Cyber-Angriffen in meinem Unternehmen um?

Interview mit Thomas Haase,
Head of Penetration Test & IT Forensik, T-Systems Multimedia Solutions

Schwachstellen in Unternehmen

Opfer eines Cyber-Angriffes zu werden, ist für viele Unternehmen ein Super-Gau. Was zeigen Ihre Erfahrungen - wie gehen Unternehmen damit um?

Viele unserer Kunden sind sich dieser Bedrohung sehr bewusst. Wir registrieren eine stetige Zunahme an Anfragen, gerade auch im Bereich IT-Forensik. Forensische Analysen helfen dort weiter, wo die interne IT an ihre Grenzen stößt. Ein IT-Forensiker beschäftigt sich mit der tiefen methodischen Analyse von IT-Vorfällen und der gerichtsverwertbaren Sicherung der Beweise. Jedoch sind gute IT-Forensiker in der Praxis ein sehr rares Gut und nicht immer macht es Sinn, diese selbst im Unternehmen vorzuhalten.

Reaktiv

Können Sie beschreiben, wie eine IT-forensische Analyse abläuft?

In vielen Fällen kommen Anrufe direkt bei der Forensik Hotline an. Nachdem der Vorfall geschildert und mit Hilfe einer Checkliste aufgenommen wurde, werden verschiedene Sofortmaßnahmen mit dem Kunden durchgegangen. Beispielsweise kann das eine Separierung der betroffenen Systeme sein oder wichtige Maßnahmen, welche spätere Beweissicherungen möglich machen.

Hierbei kommt es natürlich auf den konkreten Vorfall an. Sehr oft werden wir, wie bereits mit Ransomware dargestellt, mit sogenannten Verschlüsselungstrojanern konfrontiert. In diesen Fällen liegt ein Schwerpunkt auf der Identifikation der Schadsoftware, um die nächsten Schritte ableiten zu können. Hierzu gibt es zum Beispiel einen sogenannten Upload Service, über den der Kunde die Schadsoftware zur Analyse in unser Labor schicken kann. Hier können, nach erfolgter Analyse, die nächsten Maßnahmen entwickelt werden. Im Idealfall wird natürlich die Wiederherstellung der verschlüsselten Daten angestrebt.

Thomas Haase
Head of Penetration
Test & IT Forensik

Expertenmeinung

Alternativ wird, mit Hilfe verschiedener Vorkehrungen, versucht einerseits den Schaden einzugrenzen, wie auch einen schnellen Wiederanlauf zu ermöglichen. Ein weiterer Schwerpunkt liegt im Anschluss auf der Ableitung möglicher Maßnahmen und Learnings, damit es idealerweise nicht wieder zu einem erneuten Vorfall kommt.

Handlungsempfehlung im Notfall

Im Fall eines Angriffs ist schnelles Handeln notwendig. Wie reagiere ich richtig?

Als erstes gilt auch hier: Ruhe bewahren und fokussiert die Notfallmaßnahmen umsetzen, welche im Vorfeld definiert wurden. Auch ein Krisentraining hilft, Mitarbeiter für solche Notfälle vorzubereiten und die richtigen Maßnahmen einzuleiten. Es ist wichtig den Angriff schnellstmöglich zu lokalisieren und eine weitere Ausweitung einzugrenzen.

Wir bieten bereits über 300 Kunden einen 24 x 7 Incident Response Service an, welcher rund um die Uhr zur Verfügung steht und im Notfall sofort reagieren kann. So helfen wir auch nach einem Angriff, Licht ins Dunkle zu bringen, Systeme zu analysieren und diese schnell wieder arbeitsfähig zu bekommen.

Rund um die Uhr einsatzbereit

Wie kann der 24 x 7 Incident Response Service Unternehmen bei einem Cyber-Angriff unterstützen?

Sobald ein Vorfall in Ihrem Unternehmen erkannt wird, können Sie rund um die Uhr unsere Hotline anrufen. Nach einer Reihe von Sicherheitsvorkehrungen, welche das Schadausmaß und die Ausbreitung eindämmen sollen, identifiziert einer unserer Mitarbeiter zusammen mit dem betroffenen Unternehmen die Malware. Oft kann die Schadsoftware isoliert und die Daten doch noch gerettet werden. Analysierung möglicher Gegenmaßnahmen und die Beratung zu möglichen Sofortmaßnahmen gehört zu unserem Portfolio.

Im Anschluss schauen wir zusammen mit dem Kunden, welche Maßnahmen umgesetzt werden müssen, damit sie das nächste Mal besser vorbereitet ist.

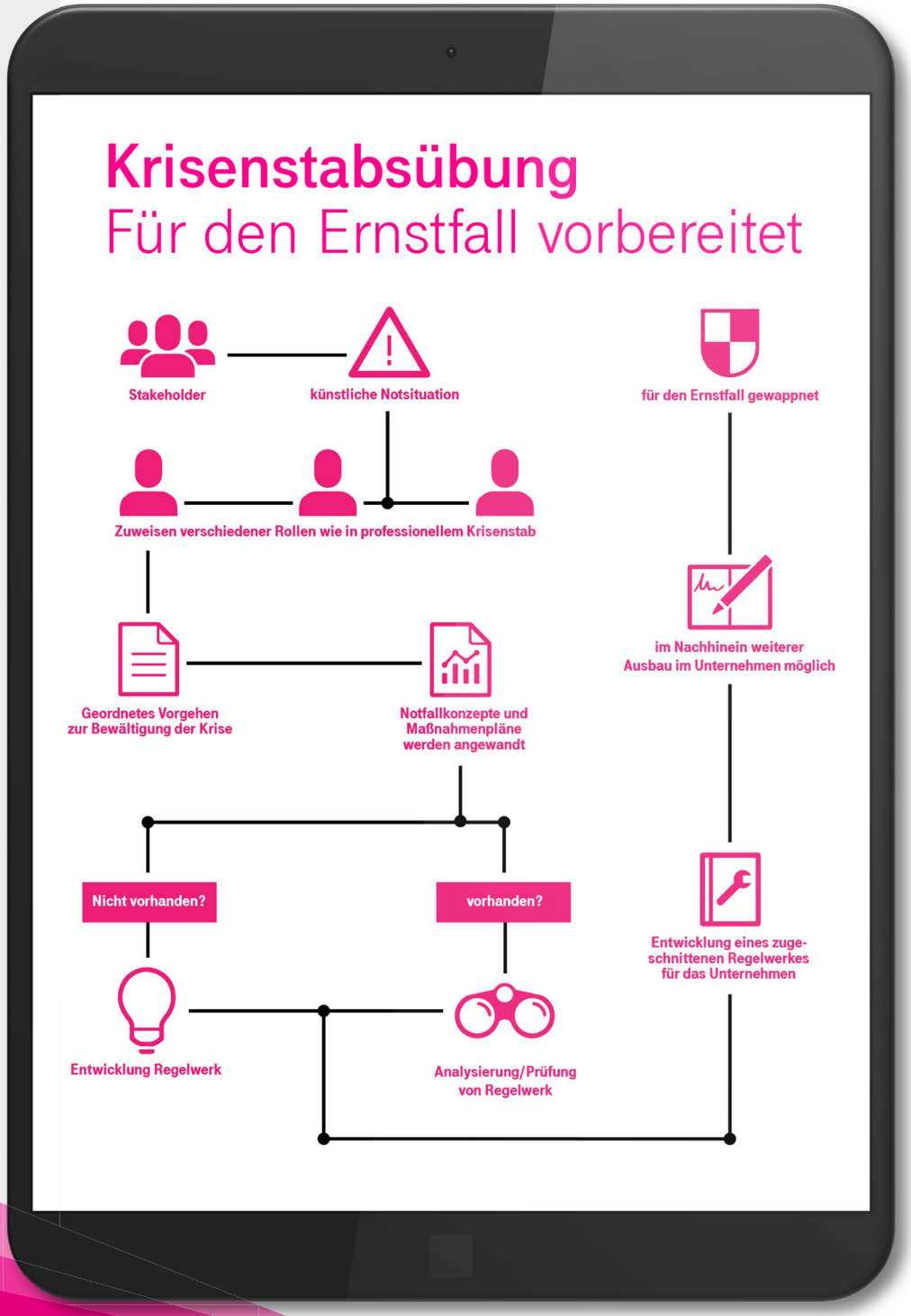
Weitere Informationen finden Sie hier.

Expertenmeinung

Gutes Krisenmanagement durch regelmäßige Trainings

Präventiv

In einer Angriffssituation tragen Notfallkonzepte und Maßnahmenpläne erst zum Schutz des Unternehmens bei, wenn diese auch professionell angewandt werden. Hier kommt die Krisenstabsübung ins wortwörtliche Spiel. Es handelt sich dabei um eine begleitete, mehrstündige Übung, die auf einem vorgefertigten Krisen-Szenario basiert.



Mitarbeiter trainieren

Expertenmeinung

Kurzum bieten derartige Krisenstabsübungen folgende Vorteile:

- praktische Anwendung definierter Rollen und Verantwortlichkeiten in der Notfallorganisation
- Trainieren eines logischen Vorgehens bei der Erschließung von geschäftskritischen Vorfällen sowie daraus resultierender Entscheidungsfindung vor dem Hintergrund einer laufenden Krise
- Anwendung von im Unternehmen vorhandener Dokumente zur Notfall- und Krisenbewältigung sowie Erkenntnisgewinn über deren Qualität
- Erarbeitung von Maßnahmen und Vorgehen
- Einüben einer angemessenen Krisenkommunikation
- Ideenfindung hinsichtlich alternativer Lösungsszenarien zur Aufrechterhaltung des Geschäftsbetriebs (z. B. Realisierung von im Normalfall digitalen Geschäftsprozessen)
- Simulation von Cyberrisiken in einem Cyber Drill hilft, diese im eigenen Unternehmen zu erkennen und zu bewerten.
- Die Notfallvorsorge wird so besser planbar. Erkannte Lücken können geschlossen werden. Dies hat zum Vorteil, dass sich im echten Notfall auf diese Lücken konzentriert werden können, die verborgen geblieben sind.

„Für viele unserer Kunden ist dieses Training sehr wertvoll. Alle Beteiligten erhalten einen gleichen Kenntnisstand zu den vorliegenden Notfallmaßnahmen und wichtigen Unterlagen. Die Mitarbeiter fühlen sich dadurch für Ernstfälle gut vorbereitet."

Ute Seidel

Ute Seidel
Head of Digital
Quality Management

Sie haben Fragen zu geschäftskritischen Vorfällen?
Weitere Informationen finden Sie auf unserer Website.

T · · Systems · Let's power higher performance

Expertenmeinung

Was können Sie schon jetzt tun?

Security Check-Box

- Sein Sie skeptisch!
- Trennen Sie private und geschäftliche Daten!
- Verwenden Sie starke Passwörter!
- Verwenden Sie unterschiedliche Passwörter!
- Trennen sie private und geschäftliche Passwörter!
- Sichern Sie Ihre mobilen Geräte!
- Sichern Sie Ihre Daten!
- Halten Sie Ihre Software und Firmware aktuell!

Über T-Systems Multimedia Solutions

Die T-Systems Multimedia Solutions begleitet Großkonzerne und mittelständische Unternehmen bei der digitalen Transformation. Der Marktführer mit einem Jahresumsatz von 176 Mio. € im Jahr 2019 zeigt mit seiner Beratungs- und Technikkompetenz neue Wege und Geschäftsmodelle in den Bereichen Industrial IoT, Customer Experience, New Work sowie Digitale Zuverlässigkeit auf. Mit rund 2100 Mitarbeitern an sieben Standorten bietet der Digitaldienstleister ein dynamisches Web- und Application-Management und sorgt mit einem akkreditierten Test-Center für höchste Softwarequalität, Barrierefreiheit und IT-Sicherheit.

Ausgezeichnet wurde T-Systems Multimedia Solutions mehrfach mit dem Social Business Leader Award der Experton Group sowie dem iF Design Award und gehörte 2017 zu den Gewinnern des Outstanding Security Performance Awards. Zudem wurde das Unternehmen mit Hauptsitz in Dresden mehrmals als einer von Deutschlands besten Arbeitgebern mit dem Great Place to Work Award gekürt sowie als „Bester Berater 2020“ vom Wirtschaftsmagazin brand eins ausgezeichnet.

Weitere Informationen: **www.t-systems-mms.com**