Incident Response zur Prävention

Warum Unternehmen in Deutschland schlecht auf Cyberangriffe vorbereitet sind und wie sie dank Incident-Response-Methoden cyberresilienter werden

kaspersky BRING ON THE FUTURE

kaspersky.de

„Die (Nicht-) Vorbereitung auf Angriffe vieler Unternehmen in Deutschland ist besorgniserregend. Seit Jahren zeigen immer wieder große Angriffe, wie wichtig es ist, umfassende Sicherheitsmaßnahmen implementiert zu haben und vorbereitet zu sein, um im Falle des Falles schnell reagieren zu können. Jedoch ist noch allzu oft das Gegenteil der Fall: Unternehmen scheuen Kosten und Aufwand, entsprechende Incident-Response-Pläne zu entwickeln, die ihnen im Notfall helfen können, schnell und effizient zu reagieren. Das muss sich ändern!"

Kai Schuricht,
Lead Incident Response Specialist
bei Kaspersky

Methodologie
Die Umfrage wurde von Arlington Research im Auftrag von Kaspersky im Juni 2023 durchgeführt. Dabei wurden insgesamt 200 IT-Entscheidungsträger in Deutschland, 50 in Österreich und 50 in der Schweiz zum Thema Incident Response und Cybersicherheit befragt.

Inhaltsverzeichnis

Top-5-Ergebnisse

- **Es fehlt an grundlegenden Sicherheitsmaßnahmen:** Nur 64,5 Prozent haben eine Passwort-Richtlinie, die kontrolliert wird; lediglich 58,0 Prozent erstellen regelmäßig Backups und nur 14,5 Prozent führen Angriffssimulationen durch
- **Incident Response? Teilweise Ahnungslosigkeit:** Nur 62,0 Prozent der Entscheider wissen, was Incident-Response-Services und -Tools sind. Nur 20,5 Prozent der Unternehmen verfügen über Incident-Response-Pläne.
- **Falsche Prioritäten:** 41,0 Prozent sehen in der Erstellung von Incident-Response-Plänen eine Zeit- und Geldverschwendung
- **Zu wenig Vertrauen ins eigene Team:** 40,0 Prozent denken, dass das eigene Security-Team das Risiko, das von einem Angriff ausgeht, nicht einschätzen kann
- **Mitarbeitern droht Kündigung bei Fehlverhalten,** laut Aussage einiger Entscheider

Waldemar Bergstreiser,
General Manager Central Europe
bei Kaspersky

Vorwort: Incident Response – Im Ernstfall richtig gewappnet sein

Spear Phishing, Ransomware, DDoS-Attacken, Spyware, generische Malware, aber auch zielgerichtete Angriffe – Unternehmen jeder Größenordnung sehen sich tagtäglich mit einer Vielzahl von Cyberbedrohungen konfrontiert. Die Konsequenzen eines erfolgreichen Cyberangriffs können dabei verheerend sein: neben Diebstahl und dem Verkauf sensibler Kunden- oder Betriebsdaten, Ruf- und Imageschädigung, der Unterbrechung des Geschäftsbetriebs sowie finanziellen Verlusten kann es schlimmstenfalls auch die Schließung des betroffenen Betriebs bedeuten.

Laut TÜV-Verband hatten Entscheider in jeder neunten Finanzorganisation im vergangenen Jahr einen Sicherheitsvorfall zu beklagen. Auch der Bitkom e. V. meldete im Jahr 2022, dass ein Schaden von etwa 203 Milliarden Euro pro Jahr durch Cyberangriffe auf deutsche Unternehmen zurückzuführen ist.

Unabhängig ob im Mittelstand oder Großkonzern, Entscheidungsträgern sollte klar sein, dass eine präventive und nachhaltige Cybersicherheitsstrategie das A und O für Cyberschutz ist. Schließlich sind nicht ausreichend geschützte Unternehmensdaten und -systeme für Cyberkriminelle die ideale Grundlage, um eine Cyberattacke zu initiieren. Wurde eine Schwachstelle in einem Netzwerk von Cyberkriminellen als Einfallstor für einen Cyberangriff ausgenutzt, muss ein Unternehmen gleich zwei Herausforderungen lösen: Einerseits den entstandenen Schaden schnellstens erkennen, analysieren und minimieren und andererseits den geschäftlichen Betrieb entweder unter den widrigen Umständen aufrechterhalten oder wieder möglichst zeitig aufnehmen.

Es liegt an der Führungsetage eines Unternehmens, vorab und gemeinsam mit den Sicherheitsteams die Vorgehensweise des Unternehmens bei einem Cybervorfall und dessen möglichen Folgen festzulegen, Stichwort: Incident Response (IR). IR beschreibt die Maßnahmen, um die Vorfallreaktionen einzuleiten, nachdem potenziell schädliche Aktivitäten im Netzwerk festgestellt wurden. Voraussetzung dafür ist die Ausarbeitung eines formellen Incident-Response-Plans. In diesem werden Zuständigkeiten festgelegt und Schritt für Schritt geklärt, wann und wie Cybersicherheitsteams auf verschiedene Angriffsarten reagieren und welche Maßnahmen sie zur Identifizierung und Behebung von Vorfällen einleiten müssen.

In vielen Unternehmen gibt es bezüglich der Erkennungsmethoden und der Verfahren zur Reaktion auf Cybersicherheitsvorfälle durchaus Raum für Verbesserungen. Denn je früher eine Organisation auf einen Angriff reagiert, desto geringer sind die damit zusammenhängenden schädlichen Folgen.

Cybersicherheitsstrategien, -tools und -dienste aus dem Bereich Incident Response können genau dies leisten: die Cybersicherheit eines Unternehmens insgesamt stärken, indem der Status quo analysiert, Schwachstellen beseitigt und ein genauer Plan für die Reaktion auf Vorfälle erstellt wird. IR umfasst nicht nur Maßnahmen im Falle eines Incident, sondern stellt vielmehr einen fortlaufenden Prozess aktiver und präventiver Maßnahmen dar, die zu einer immer höheren allgemeinen Cybersicherheit führen.

Dieser Report präsentiert den aktuellen Stand der Cybersicherheit in Unternehmen in Deutschland mit einem spezifischen Fokus auf die Vorteile eines präventiven Einsatzes von IR-Praktiken und -Tools. Entscheidungsträger erhalten einen umfassenden Überblick zum Thema sowie eine praktische Anleitung für die Erstellung eines Incident-Response-Playbooks. Ein grundlegender Schritt hin zu mehr Cyberresilienz!

Was ist eigentlich Incident Response?

Wird ein Unternehmen angegriffen, steht dieses vor zwei Herausforderungen, die gelöst werden müssen. Zum einen, muss der Schaden minimiert und zum anderen so schnell wie möglich zum normalen Arbeitsablauf zurückgekehrt werden. Hier kommt Incident Response ins Spiel, sie reagiert auf einen Sicherheitsvorfall (Vorfallreaktion); aber nicht nur das. Sie liefert ein detailliertes Bild des Vorfalls. Ein Incident-Response-Service wie der von Kaspersky deckt den gesamten Untersuchungs- und Reaktionszyklus von Vorfällen ab: von der frühen Reaktion auf Vorfälle und der Sammlung von Beweismitteln bis hin zur Identifizierung zusätzlicher Spuren von Hackerangriffen und der Erstellung eines Plans zur Angriffsabwehr.

Generell besteht Incident Response aus sechs Phasen:

- **Vorbereitung:** Incident Response sollte nicht nur als proaktive Reaktion auf einen Sicherheitsvorfall verstanden werden, sondern auch als präventive Maßnahme. Unternehmen bereiten sich allgemein auf den Ernstfall vor. Dazu gehören unter anderem Incident-Response-Pläne und -Playbooks, Table Top Exercises oder das Abschließen einer dedizierten Cyberversicherung.
- **Erkennung:** In dieser Phase wird ein Vorfall als solcher identifiziert und gemeldet sowie die ersten Informationen zum Vorfall gesammelt.
- **Schadensbegrenzung:** Basierend auf den vorhandenen Informationen wird der Vorfall eingedämmt, damit sich dieser nicht weiter im Unternehmensnetzwerk ausbreiten kann.
- **Beseitigung:** Mit der Schadensbegrenzung geht die Beseitigung des Angriffs einher. Vorhandene Schaddateien werden von den infizierten Geräten entfernt, die Systeme werden mit weiteren Sicherheitsmaßnahmen gehärtet, Updates werden eingespielt und vorhandene Sicherheitslücken geschlossen.
- **Wiederherstellung:** In dieser Phase werden die Systeme wiederhergestellt, nachdem diese beispielsweise von der Infrastruktur getrennt wurden. Backups werden wieder eingespielt.
- **Lessons Learned:** Nach dem Angriff ist vor dem Angriff. Nach einem Angriff werden alle unternommenen Schritte durchgegangen und rückblickend analysiert: Was lief gut? Was lief schlecht? Basierend auf diesen Informationen werden dann die vorhandenen Incident-Response-Pläne, -Playbooks oder -Checklisten aktualisiert (s. Punkt eins dieser Liste „Vorbereitung“).

37,0 Prozent der Unternehmen schulen ihre Mitarbeiter nicht regelmäßig zu den Themen wie Spam oder Phishing.

42,0 Prozent der Unternehmen führen keine regelmäßige Datensicherung durch.

Unternehmen in Deutschland sind nicht für aktuelle Sicherheitsherausforderungen gewappnet

Die aktuelle Umfrage von Kaspersky unter 200 IT-Entscheidungsträger in Deutschland zeigt, dass ein Großteil der Unternehmen in Deutschland weder für die aktuellen Sicherheitsherausforderungen gewappnet ist noch die Anforderungen der NIS2 erfüllt. Mehr als ein Drittel (35,5 Prozent) der Unternehmen hat keine Richtlinie für sichere Passwörter oder kontrolliert deren Einhaltung nicht. Unsichere Passwörter machen es Angreifern leichter, in ein Netzwerk einzudringen und Ransomware oder andere Schadsoftware einzuschleusen.

Besorgniserregend ist zudem, dass 37,0 Prozent der Unternehmen ihre Mitarbeiter nicht regelmäßig zu den Themen wie Spam oder Phishing schulen – klassische Einfallstore von Cyberkriminellen, um an Zugangsdaten zu gelangen. Die Zeiten schlecht geschriebener Spam- und Phishing-Mails voller Rechtschreibfehler sind längst vorbei. Spam- oder Phishing-E-Mails sind heute kaum noch von echten Nachrichten zu unterscheiden. Jedoch setzt nur etwas mehr als die Hälfte (54,5 Prozent) der Unternehmen Anti-Phishing-Software ein. Angesichts der aktuellen Sicherheitslage und einer recht konstant hohen Anzahl an Phishing-Angriffen setzen sich Unternehmen damit der Gefahr eines Ransomware-Angriffs aus.

Ein weiteres Risiko: 42,0 Prozent der Unternehmen führen keine regelmäßige Datensicherung durch. Das heißt im Falle eines Ransomware-Angriffs – oder sei es auch die Zerstörung der physischen Datenträger – ist der Zugriff auf die Daten nicht mehr möglich.

„Dass viele Unternehmen immer noch nicht regelmäßige Datensicherungen durchführen, ist kaum zu glauben“, so Kai Schuricht, Lead Incident Response Specialist bei Kaspersky. „Kommt dann noch die Kombination aus unsicheren Passwörtern und ungeschulten Mitarbeitern hinzu, kann Ransomware ein Unternehmen schnell an die Grenzen der wirtschaftlichen Belastbarkeit bringen. Die Gefahr eines erfolgreichen Angriffs ist in diesem Fall besonders hoch.“

Präventive Incident Response? Fehlt in vielen Unternehmen

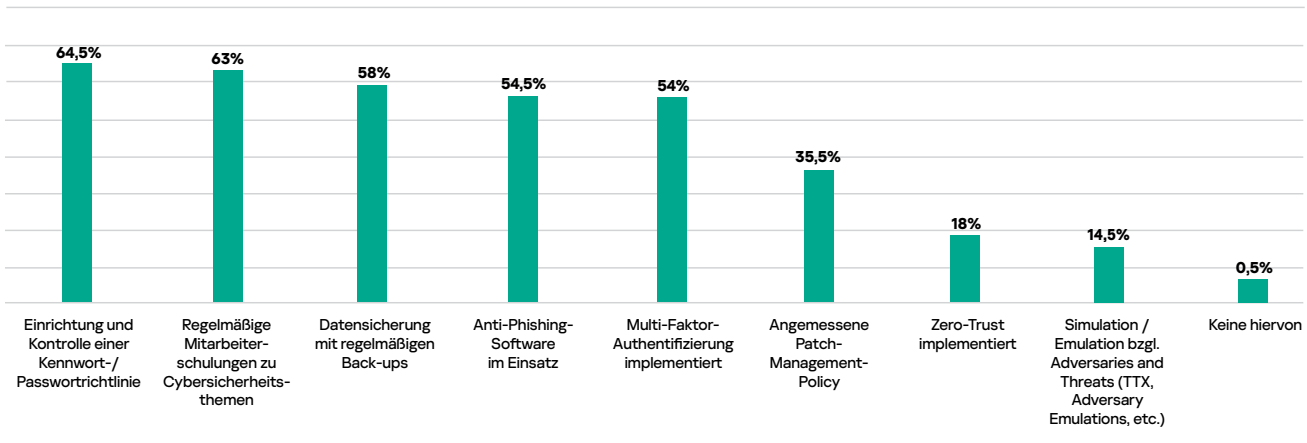
Der Status quo an Sicherheitsmaßnahmen bei einigen Unternehmen in Deutschland ist ernüchternd, wenn man sich die Ergebnisse der aktuellen Kaspersky-Umfrage detailliert ansieht. Grundlegendste Dinge, wie Passwort-Richtlinien, Backup-Erstellung oder Multi-Faktor-Authentifizierung, sollten neben einem effektiven Endpoint-Schutz zum absoluten Basisschutz gehören. Allerdings sieht die Realität anders aus: diese sind nur in 64,5 Prozent beziehungsweise 58,0 Prozent und 54,0 Prozent der Unternehmen vorhanden.

Nur 53,5 Prozent aller befragten Unternehmen in Deutschland verwendet Richtlinien, wie Sicherheitsvorfälle zu dokumentieren sind.

Wenn es um „fortgeschrittene Maßnahmen" gegen fortgeschrittene Angriffe geht, ergibt sich ein ähnliches Bild. Die aktuelle Kaspersky-Umfrage zeigt, dass nur die Hälfte (53,5 Prozent) aller befragten Unternehmen in Deutschland Richtlinien verwendet, wie Sicherheitsvorfälle zu dokumentieren sind. Das wäre die erste Grundlage, um ein Incident-Response-Playbook zu erstellen. Ebenso viele Unternehmen (53,0 Prozent) haben eine definierte Stelle für die Meldung von Vorfällen. Weniger als die Hälfte der Unternehmen (47,5 Prozent) nutzt Netzwerksegmentierung, um Geräte voneinander abzuschotten und nur 37,5 Prozent setzen Tools zur ersten Analyse von Sicherheitsvorfällen ein. Noch weniger (34,5 Prozent) führen präventive Audits durch.

85,5 Prozent der Unternehmen führen keine Simulation / Emulation in Bezug auf Adversaries and Threats (via Table Top Exercise (TTX) oder Adversary Emulations) durch. Ohne das Testen kritischer Prozesse können Unternehmen jedoch nicht davon ausgehen, dass diese im Ernstfall eine Hilfe sind und Orientierung bieten. Es ist wenig ratsam, sich blind auf die Funktionsfähigkeit einzelner Komponenten der Sicherheitsinfrastruktur zu verlassen, ohne diese Dienste und Prozesse durch Simulationen auch regelmäßig zu testen. Denn Notfallpläne und Meldeketten sind nur dann verlässlich, wenn auch sicher ist, dass diese reibungslos und wie geplant im Notfall funktionieren.

Zur Vorbeugung von Cybersicherheitsvorfällen haben wir folgende Maßnahmen im Unternehmen implementiert: (Mehrfachauswahl)



Nur 20,5 Prozent der Unternehmen in Deutschland verfügen über Incident-Response-Pläne.

29,0 Prozent haben ein Incident-Response-Playbook.

30,5 Prozent der Unternehmen in Deutschland verfügen über eine Cyberversicherung, die im Schadensfall die gröbsten Kosten abdeckt. Bedenklich ist jedoch, dass nur 20,5 Prozent der Unternehmen über Incident-Response-Pläne verfügen, obwohl dies für die meisten Cyberversicherungen obligatorisch ist. Weniger als ein Drittel (29,0 Prozent) der befragten Unternehmen verfügt über ein Incident-Response-Playbook. 26,5 Prozent der Unternehmen haben eine zentral dokumentierte Ablage für kompromittierte Geräte. Diese ist für die Forensik wichtig, da nur so der Ursprung eines Angriffs identifiziert werden kann. Im Umkehrschluss bedeutet das aber auch, dass dreiviertel der Unternehmen keine Ablage nutzen. Das macht das Nachvollziehen des Angriffs und die Beseitigung dessen Schäden sehr viel schwieriger.

Ein Incident-Response-Playbook definiert die Maßnahmen, die Unternehmen im Falle eines bestimmten Vorfalls ergreifen sollte. Ein Incident-Response-Plan ist hingegen auf eine Vielzahl von Vorfällen anwendbar. Pläne zur Vorfallreaktion sollen dabei helfen, ein Mitglied eines Unternehmens anleiten.

Derzeit verfügt nur jedes dritte Unternehmen (35,5 Prozent) über eine Patch-Management-Richtlinie. Dabei gehören Sicherheitslücken in Anwendungen und Betriebssystemen zu den häufigsten Angriffsvektoren in Unternehmen. In Verbindung mit Phishing-Angriffen können Cyberkriminelle so Daten aus Netzwerken stehlen, Unternehmen erpressen, lokal betriebene Server und Rechner kompromittieren, in Botnetze einbinden und viele weitere schädliche Aktionen durchführen. Der Kaspersky Incident Response Analyst Report zeigt, dass ein zeitnahes Patch-Management unerlässlich ist.

„Patchen ist immer eine Herausforderung. Zum einen lassen sich zwar Sicherheitslücken relativ einfach stopfen, zum anderen ist der Vorgang aber meist etwas komplizierter als man denkt“, sagt Kai Schuricht, Lead Incident Response Specialist bei Kaspersky, zum fehlenden Patch-Management in Unternehmen. „Entscheiden sich Unternehmen, ihre Systeme zu aktualisieren, dauert dies einige Zeit. Denn diese müssen erst getestet, freigegeben und dann verteilt werden. Das dauert und vergrößert natürlich das Zeitfenster, in dem die Systeme verwundbar sind. Auch das Zeitfenster für erfolgreiche Angriffe verlängert sich. Ein entsprechend durchdachtes und damit effizientes Patch-Management kann hier unterstützen und die unterschiedlichen Anforderungen von beispielsweise IT-Sicherheit und Produktion gleichzeitig berücksichtigen.“

Weiterhin nutzen nur 18,0 Prozent aller Unternehmen den Zero-Trust-Ansatz, bei dem Nutzer und Administratoren nur diejenigen Rechte erhalten, die sie auch tatsächlich in ihrer Rolle und bei ihrer Arbeit benötigen. Gleichzeitig ist sichergestellt, dass Authentifizierung und Sicherheitsprüfungen so oft wie möglich stattfinden. Gelangen Angreifer in einer Umgebung ohne Zero-Trust an Zugangsdaten, können sie sich viel leichter im Netzwerk bewegen und ungestörter Systeme kompromittieren. Dies scheint, laut Umfrageergebnisse, aktuell bei über 82,0 Prozent der Unternehmen in Deutschland möglich.

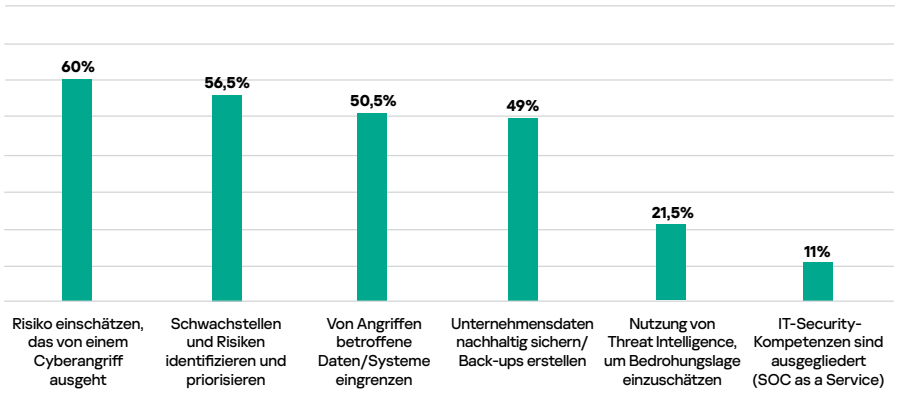
Von Vertrauen und Selbstüberschätzung – Sind die IT-Entscheider das Problem?

Die aktuelle Kaspersky-Umfrage zeigt, dass viele IT-Entscheider zu wenig Vertrauen in ihr eigenes Sicherheitsteam haben, wenn es um die Einschätzung von Risiken und Bedrohungen im Cyber-Universum geht. Da hilft es auch nicht, dass die eigenen Mitarbeiterinnen und Mitarbeiter bei Fehlern unter Umständen sogar mit empfindlichen Konsequenzen, bis hin zur Entlassung – laut Aussage einiger Befragter – rechnen müssen.

Laut Umfrage glauben 40,0 Prozent der Entscheider nicht, dass das eigene Sicherheitsteam das Risiko, das von Angriffen ausgeht, richtig einschätzen kann. Incident-Response-Pläne, in denen klar beschrieben und damit definiert ist, wann welche Situation eintritt und eventuell wie diese eskaliert werden muss, bieten eine gute Orientierung für Sicherheitsteam und Entscheider. Außerdem stehen damit schon im Vorneherein abgesprochene Handlungsoptionen offen, wie auf Risiken und Angriffe zu reagieren ist. Das schafft Vertrauen und Handlungssicherheit.

Nur etwas mehr als die Hälfte der befragten IT-Entscheider (56,5 Prozent) trauen ihrem Team zu, Schwachstellen und Risiken richtig zu identifizieren und zu priorisieren. Ebenso wenige (50,5 Prozent) vertrauen ihrem Team, die betroffenen Systeme zu isolieren. Weniger als die Hälfte (49,0 Prozent) der IT-Verantwortlichen im Unternehmen glaubt außerdem, dass ihr Team in der Lage sei, Backups korrekt durchzuführen.

In welchen der folgenden Bereiche würden Sie Ihr Team als sehr kompetent einschätzen? (Mehrfachauswahl)



IT-Entscheider sind recht optimistisch, wenn es um die schnelle Erkennung von Sicherheitsvorfällen geht. 41,5 Prozent der IT-Entscheider gehen sogar davon aus, dass Sicherheitsvorfälle innerhalb weniger Minuten entdeckt werden; 40,5 Prozent glauben, dass dies innerhalb weniger Stunden der Fall sei. Beide Ergebnisse zeigen eine Zuversicht, die angesichts der Möglichkeiten moderner Cyberangriffe sowie deren Zielsetzung möglichst unauffällig zu agieren, eher unwahrscheinlich ist.

Diese Vermutung wird durch die Erkenntnisse des Kaspersky Incident Response Analyst Report belegt: Die meisten Fälle, in denen der ursprüngliche Zugriff nicht erkannt wurde, dauerten mehr als ein Jahr, bevor sie von der Organisation entdeckt wurden, da zu diesem Zeitpunkt aufgrund von Protokollrotationsrichtlinien keine Artefakte mehr zur Analyse vorhanden waren. Mehr als die Hälfte aller Angriffe, die mit bösartigen E-Mails, gestohlenen Anmeldedaten und der Ausnutzung externer Anwendungen begannen, wurden hingegen innerhalb von Stunden oder Tagen entdeckt.

Ein ähnliches Bild ergibt sich bei der Selbsteinschätzung, wie lange es dauert, einen Angriff einzudämmen beziehungsweise Malware zu beseitigen. Während 25,0 Prozent der Entscheider der Meinung sind, dies könne innerhalb von Minuten geschehen, teilt Kai Schuricht diese Ansicht nicht. Er stellt aus seiner langjährigen Erfahrung fest: „Das ist mehr als sportlich!“ Denn schon allein die Untersuchung eines Angriffs, der länger als eine Woche dauerte, nimmt durchschnittlich über 60 Stunden in Anspruch.

Fehlerkultur: Verständnis und Schulung oder Tadel und Konsequenzen?

Zwar sagen zwei Drittel (67,5 Prozent) der Befragten, sie hätten eine gute Fehlerkultur in ihrem Unternehmen, jedoch stimmen nur 19,5 Prozent aller Umfrageteilnehmer voll und ganz zu, dass Mitarbeiter keine Konsequenzen zu befürchten hätten. Bei einigen Unternehmen drohen Mitarbeitern, die auf eine Phishing-E-Mail hereinfallen oder auf einen Malware-Link klicken, sogar drastische Konsequenzen. In den Antworten der Befragten tauchen häufig die Aussagen „wird gefeuert“, „bekommt eine Abmahnung“ oder „das ist nicht schlau“ auf.

„Eine gute Fehlerkultur im Unternehmen ist essenziell, damit Mitarbeiter Sicherheitsvorfälle sofort melden, denn bei einem IT-Sicherheitsvorfall kommt es auf eine schnelle Reaktion an“, erklärt Kai Schuricht, Lead Incident Response Specialist bei Kaspersky. „Wenn Mitarbeiter mit Konsequenzen rechnen müssen, ist die Wahrscheinlichkeit hoch, dass sie Vorfälle unterschätzen oder verschweigen. Allerdings ist es wichtig, dass Verantwortliche zeitnah über Fehlverhalten oder Fehler informiert werden, um den Schaden so gering wie möglich zu halten, indem effizient auf die Attacke reagiert wird.“

Zwischen Vorbereitung und Fahrlässigkeit – Vorfallreaktionskapazität: mangelhaft

61,5 Prozent der Befragten in Deutschland setzen Incident-Response-Pläne und -Tools ein.

38,0 Prozent wissen nicht, was Incident-Response-Tools sind.

Immerhin 61,5 Prozent der Befragten setzen Incident-Response-Pläne und -Tools ein und sind der Meinung, dass IR-Dienste und -Tools in der Vergangenheit schon Angriffe verhindert hätten. Ähnlich viele (60,5 Prozent) simulieren Vorfälle und testen ihre IR-Pläne regelmäßig.

„Wenn Unternehmen gut auf Angriffe vorbereitet sind, kann ein Großteil der Cyberattacken verhindert werden“, so Kai Schuricht, Lead Incident Response Specialist bei Kaspersky. „Die häufigsten Angriffsvektoren sind öffentlich zugängliche Anwendungen, kompromittierte Accounts und schädliche E-Mails. Diese lassen sich durch rechtzeitiges Patch-Management, die Einführung von Multi-Faktor-Authentifizierung, Lösungen mit Anti-Phishing-Software zur Abwehr von Phishing-Angriffen sowie regelmäßige Mitarbeiterschulungen jedoch recht einfach schützen.“

Und obwohl die Teilnehmer der Kaspersky-Umfrage die Verantwortung für die Cybersicherheit in ihrem Unternehmen tragen, scheinen viele nicht zu wissen, wie wichtig Incident-Response-Pläne sind und wie moderne Angriffe genau ablaufen. Da dieses Wissen fehlt, bereiten sich viele Unternehmen vermutlich nicht genügend auf moderne Cyberangriffe vor und sind in der Folge weniger cyberresilient. 38,0 Prozent der Befragten wissen nicht, was Incident-Response-Tools sind und welche Möglichkeiten sie bieten. Dies zeigt einen großen Nachholbedarf bei vielen Unternehmen in Deutschland.

Weiterhin kennt zwar in etwa die Hälfte der Befragten (44,5 Prozent) die Bedeutung entsprechender Incident-Response-Tools, setzt sie jedoch nur im Notfall ein und bewertet sie nicht unbedingt als Teil einer präventiven Schutzstrategie. 41,0 Prozent sind gar der Ansicht, dass IR-Pläne keinen Nutzen hätten und beurteilen deren Erstellung als reine Zeit- und Geldverschwendung.

„Auch bei Cyberangriffen gilt: besser Vorsorge als Nachsorge. Heißt: Unternehmen sollten bereits vor einem Vorfall präventiv in Maßnahmen investieren und nicht erst, wenn ein akuter Angriff vorliegt“, so Kai Schuricht, Lead Incident Response Specialist bei Kaspersky. „Dabei ist die Erstellung von IR-Plänen gar nicht so kompliziert. Im Internet gibt es sogar kostenlose Templates, beispielsweise unter https://www.incidentresponse.org/playbooks/; und auch das BSI unterstützt mit Vorlagen, die einfach auszufüllen sind.“

Beispiel einer Struktur eines Incident-Response-Plans:

- **Übersicht Incident-Reponse-Plan**
- **Incident Taxonomy:**
  - Klare Definition
    - „Was ist ein Information Security Incident“?
- **Incident Prioritization** (Die Priorität eines Vorfalls wird anhand der möglichen Auswirkungen auf die folgenden Einrichtungen definiert)
  - Geschäftsprozesse
  - Sensible Daten
  - Vorschritt des Angreifers (gained control)
  - Klare Definition der „Incident Priority Level”
    - Critical 1, 2, 3, 4 (mehr oder weniger abhängig vom Kunden)
- **Zuordnung der Auswirkungen eines Vorfalls zu den Prioritätsstufen eines Vorfalls**
- **Incident Kategorien:**
  - Phishing
  - Malware Outbreak
  - Etc.
- **Incident Response Team Level**
- **Incident Response RACI Matrix**
- **Mapping von Incident Response und Cyber Crisis Management Plan (CCMP)**
- **Incident Metriken und Incident Response SLAs:**
  - Definierte Zeiten für unterschiedliche Tasks im IR-Plan.

Wie man ein Incident-Response-Playbook erstellt

Ein Playbook soll dem Sicherheitsteam eines Unternehmens die Möglichkeit geben, effektiv und zeitnah auf Cyberangriffe zu reagieren. Je nach Organisation besteht der Incident-Response-Prozess aus verschiedenen Phasen. Nach NIST sind das: Vorbereitung, Erkennung und Analyse, Eindämmung, Beseitigung und Wiederherstellung sowie Aktivitäten nach einem Vorfall. Diese Zyklen können in „Aktionsblöcke" unterteilt werden. Diese Blöcke können wiederum je nach spezifischem Angriff kombiniert werden, um rechtzeitig und effizient darauf zu reagieren. Jede „Aktion" ist eine einfache Anweisung, die ein Analyst oder ein automatisiertes Skript im Falle eines Angriffs befolgt.

Schritt 1: Vorfallreaktion vorbereiten

Die erste Stufe jedes Incident-Response-Playbooks befasst sich mit der Vorbereitungsphase des NIST Incident Response Life Cycle – es geht um die Reaktion auf Vorfälle. In der Regel beinhaltet diese eine Vielzahl verschiedener Schritte, etwa die Vorbeugung von Vorfällen (Schwachstellen-Management, Sensibilisierung der Anwender oder Malware-Prävention). Das Alert-Field-Set und seine visuelle Darstellung werden definiert. Für jeden Vorfall-Typus sollten verschiedene Field-Sets vorbereitet werden, die für das Incident-Response-Team am praktikabelsten sind. Hierfür werden für eine bestimmte Art von Vorfall spezifische Rollen sowie Eskalationsszenarien und die Zuweisung der Tools für die Kontaktaufnahme mit den Stakeholdern – etwa via E-Mail, Telefon, WhatsApp oder SMS – festgelegt. Darüber hinaus benötigt das Incident-Response-Team einen angemessenen Zugang zu Sicherheits- und IT-Systemen, Analysesoftware und Ressourcen. Um eine rechtzeitige Reaktion zu gewährleisten und menschliche Fehler zu vermeiden, bietet es sich an, Automatisierungen und Integrationen zu entwickeln und zu implementieren, die von einem Security Orchestration, Automation and Response (SOAR)-System gestartet werden können.

In der Erkennungsphase werden Daten von IT-Systemen und Sicherheitstools, öffentlich zugängliche sowie von Personen innerhalb und außerhalb des Unternehmens erhobene Informationen gesammelt und Vorstufen sowie Indikatoren identifiziert.

Schritt 2: Einen umfassenden Untersuchungsprozess etablieren

Danach folgt die Analyse, bei der Dokumentation, Triage, Untersuchung und Benachrichtigung zu berücksichtigen sind. Die Dokumentation hilft dem Team, die Analysefelder zu definieren und festzulegen, wie diese nach Entdeckung und Registrierung im Vorfallmanagementsystem ausgestaltet werden sollen. Erst danach geht das Incident-Response-Team zur Triage über, um eine Priorisierung des Vorfalls vorzunehmen, ihn zu kategorisieren, auf Falschmeldungen hin zu überprüfen sowie um nach verwandten Vorfällen Ausschau zu halten.

Den Hauptteil der Analysephase nimmt die Untersuchung – bestehend aus dem Sammeln von Protokollen, Assets und der Anreicherung von Artefakten sowie der Festlegung eines Vorfallbereichs – in Anspruch. Hier müssen alle Daten über den Vorfall vorliegen, um Patient Zero und Einstiegspunkt zu identifizieren. Das Team muss wissen, wie ein Angreifer unberechtigten Zugriff erhalten hat und welcher Host oder Account zuerst kompromittiert wurde. Dies hilft bei der Eindämmung des Cyberangriffs und der Vermeidung ähnlicher Attacken in der Zukunft. Durch das Sammeln von Vorfalldaten erhalten die Verantwortlichen relevante Informationen – etwa Assets und Artefakte wie Hostname, IP-Adresse, Datei-Hash oder URL – die mit dem Vorfall in Verbindung stehen. Der Vorfallbereich kann so entsprechend um diese ergänzt werden.

Wird der Vorfallbereich erweitert, kann das Team die Assets und Artefakte mit Daten aus Threat-Intelligence-Ressourcen oder lokalen Systemen mit Inventarinformationen wie Active Directory, IDM oder CMDB anreichern. Mithilfe eines umfassenden Überblicks zu betroffenen Ressourcen kann das Incident-Response-Team eine Risikoeinschätzung abgeben und auf deren Basis die richtigen Folgemaßnahmen ausarbeiten. Entscheidend ist dabei, wie viele Hosts, Anwender, Systeme, Geschäftsprozesse oder Kunden betroffen sind, wobei es mehrere Möglichkeiten gibt, dies zu eskalieren. Bei einem mittleren Risiko müssen nur der SOC-Manager und einige Administratoren benachrichtigt werden, um den Vorfall einzudämmen. Wird das Risiko eines Vorfalls jedoch als kritisch eingestuft, muss das Incident-Response-Team das Krisenteam, die Personalabteilung oder die Aufsichtsbehörde in Kenntnis setzen.

Diese Benachrichtigung schließt die Analysephase ab. Alle Beteiligten sollten über den aufgetretenen Vorfall schnellstmöglich informiert werden, sodass der jeweilige System Owner wirksame Eindämmungs- und Wiederherstellungsmaßnahmen ergreifen kann.

Schritt 3: Eindämmen, beseitigen, wiederherstellen

Die dritte Phase umfasst Maßnahmen zur Eindämmung, Beseitigung und Wiederherstellung. Das Hauptziel der Eindämmung besteht darin, die Situation nach einem Vorfall unter Kontrolle zu halten. Auf Grundlage der Schwere eines Vorfalls und des möglicherweise verursachten Schadens sollte das Einsatzteam zunächst geeignete Maßnahmen zur Eindämmung treffen. Nach der Vorphase, in der Arbeitsabläufe definiert wurden, liegt nun eine Liste verschiedener Objekttypen und möglicher Aktionen vor, die mit dem besprochenen Instrumentarium durchgeführt werden können. Nun müssen für die dokumentierten Aktionen geeignete Maßnahmen auf Grundlage der Auswirkungen bestimmt werden. Der Gesamtschaden hängt größtenteils von dieser Phase ab, denn je reibungsloser und präziser die im Playbook definierten Aktionen ablaufen, desto schneller können gefährliche Aktivitäten blockiert und deren Folgen minimiert werden. Während des Eindämmungsprozesses kommen verschiedene Aktionen zum Einsatz, wie das Entfernen einer schädlichen Datei oder die Verhinderung deren Aktivierung, die Isolierung eines Netzwerk-Hosts, das Deaktivieren eines Accounts oder das Scannen eines Datenträgers mit einem Antivirenprogramm.

Die Auswahl der Eindämmungsmaßnahmen hängt vom potenziellen Risiko ab. Deshalb sollte das Incident-Response-Team hierbei Vorsicht walten lassen und beispielsweise nicht die Passwörter aller Konten im Unternehmen zurücksetzen, wenn sich dieses mit einem Brute-Force-Angriff konfrontiert sieht. Manchmal verfügt das Team nicht über ausreichend Möglichkeiten, um Verstöße zu verhindern, weil es keine Berechtigungen für bestimmte Systeme hat. In diesem Fall empfiehlt es sich, Aktionen entsprechend zu kennzeichnen, die externe Fachleute wie Systemadministratoren, L3-Analysten oder Support-Teams zur Durchführung und Automatisierung solcher Iterationen erforderlich machen.

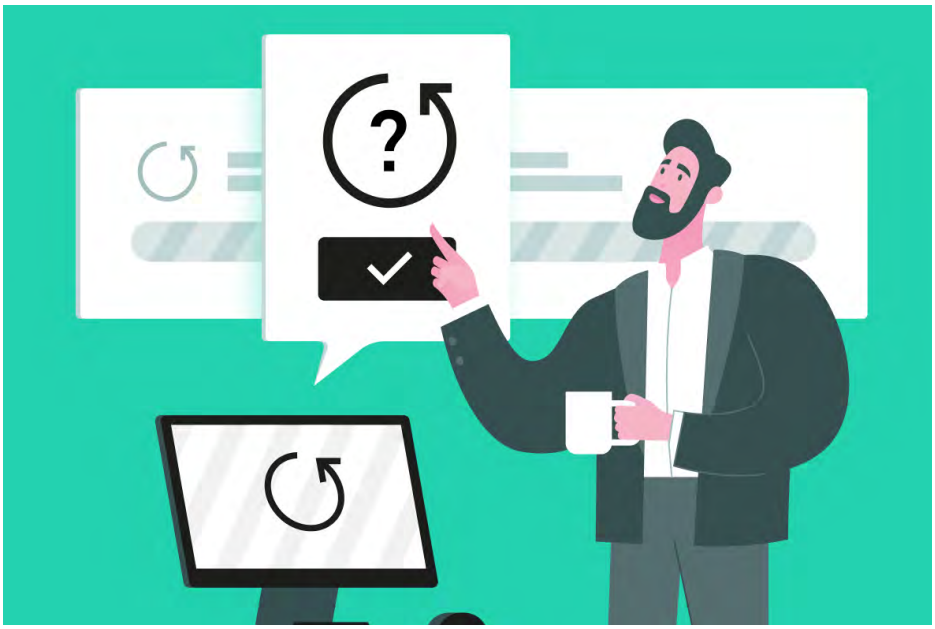
Die Phasen zur Beseitigung und Wiederherstellung bestehen aus Verfahren zur Wiederinbetriebnahme und ähneln sich in vielen Punkten. Die Bereinigung aller Anzeichen eines Angriffs, etwa schädliche Dateien oder erstellte geplante Aufgaben und Dienste, gehört zum Beseitigungsverfahren. Neben der Beseitigung ist die Wiederherstellungsphase optional, da nicht jeder Vorfall Auswirkungen auf die Infrastruktur hat. In dieser Phase sollten jedoch Health Checks durchgeführt und während des Angriffs vorgenommene Änderungen rückgängig gemacht werden.

Schritt 4: Aus dem Vorfall lernen

Die letzte Phase des Playbook umfasst die Zeit nach einem Vorfall und dem daraus resultierenden Lerneffekt. Ziel ist es, die gewonnenen Erfahrungen und Erkenntnisse für die Optimierung des gesamten Prozesses zu nutzen. Um diese Aufgabe zu vereinfachen, kann eine Reihe von Fragen definiert werden, die vom Response-Team beantwortet werden müssen:

- Wie gut ist das Incident-Response-Team mit dem Vorfall umgegangen?
- Welche Informationen wurden früher benötigt?
- Hätte das Team Informationen besser mit anderen Organisationen oder Abteilungen austauschen können?
- Was könnte das Team beim nächsten Mal anders machen, wenn sich derselbe Vorfall ereignet?
- Welche zusätzlichen Tools oder Ressourcen werden benötigt, um ähnliche Vorfälle zukünftig zu verhindern oder einzuschränken?
- Wurden falsche Maßnahmen ergriffen, die Schäden verursachten oder die Wiederherstellung behinderten?

Wurden all diese Fragen beantwortet, kann das Reaktionsteam seine Wissensbasis aktualisieren, die Erkennungs- und Präventionsmechanismen verbessern oder sogar einen neuen Reaktionsplan erarbeiten. Es entsteht ein Kreislauf aus Reaktion und präventiven Maßnahmen, der ein Unternehmen zunehmend cyberresilienter macht.



Fazit: Was muss für ein gutes IR-Playbook getan werden?

Um einen Leitfaden für die Reaktion auf Cybersicherheitsvorfälle zu entwickeln, muss der Prozess des Vorfallmanagements und seiner zugehörigen Phasen definiert werden. Dafür müssen Tools/Systeme festgelegt werden, die bei der Erkennung, Untersuchung, Eindämmung, Beseitigung und Wiederherstellung helfen. Auf Basis der gewählten Tools werden Aktionen kreiert, über die Protokolle gesammelt, Inventarinformationen oder die Telemetrie der betroffenen Assets angereichert, Hosts isoliert, der Launch schädlicher Dateien verhindert, URLs blockiert, aktive Sitzungen beendet oder Konten deaktiviert werden. Weitere Aktionen sollten sich um die Beseitigung aller Anzeichen eines Eindringens bemühen, indem Dateien aus der Ferne gelöscht, verdächtige Dienste oder geplante Aufgaben entfernt werden. Danach geht es um die Wiederherstellung des Systembetriebs, indem Änderungen rückgängig gemacht werden und gewonnenes Wissen übertragen wird.

Wichtig dabei ist, die Zuständigkeiten innerhalb des Incident-Response-Teams festzulegen und sicherzustellen, dass jeder seine spezifische Rolle genau kennt. Darauf aufbauend entstehen Prozeduren, die das Playbook bilden und im Allgemeinen wie folgt strukturiert sind: „<Ein Subjekt> führt <eine Aktion> an <einem Objekt> unter Verwendung von <einem Werkzeug> aus." Alle Subjekte, Aktionen, Objekte und Werkzeuge sind bereits definiert und sind einfach miteinander zu kombinieren. Sie bilden die einzelnen Prozesse und diese wiederum die einzelnen Elemente eines Playbooks.

Kaspersky Incident Response:
kaspersky.de/enterprise-security/incident-response

Kaspersky All-in-1-Cyberschutz:
go.kaspersky.com/All-in-1-Cyberschutz.html

Cyber Threats News: https://securelist.com/
IT-Sicherheitsnachrichten: kaspersky.de/blog/b2b/
IT-Sicherheit für KMU: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

kaspersky.de

kaspersky BRING ON THE FUTURE