sure[secure]
your security operations center

secure mag

INCIDENT RESPONSE AM DIGITALEN TATORT

Zwischen Spurensuche und Wiederaufbau

Intro

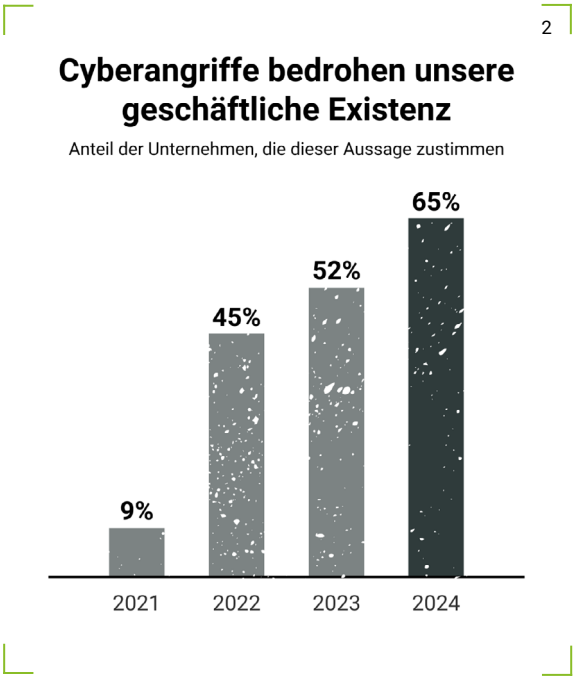
Ein Cyberangriff ist kein abstraktes Szenario, sondern ein Tatort in Echtzeit. Er hinterlässt Spuren: in Logfiles, Systemen, Entscheidungen. Doch bevor sie jemand liest, bevor klar wird, was passiert ist, vergehen oft Stunden oder Tage. In dieser Zeit entscheidet sich, ob ein Unternehmen handlungsfähig bleibt oder die Kontrolle verliert.

Cyberangriffe lassen sich nicht vollständig verhindern, **aber ihre Folgen lassen sich kontrollieren**. In einer digitalisierten Wirtschaft, in der Prozesse, Daten und Kommunikation eng miteinander verbunden sind, bedeutet ein Angriff längst mehr als eine technische Störung. Er ist eine Bewährungsprobe für Organisation, Führung und Struktur.

Ein realistischer Blick auf Incident Response

Die Zahl der Sicherheitsvorfälle steigt kontinuierlich. Laut der aktuellen Bitkom-Studie Wirtschaftsschutz 2024[1] waren in den vergangenen zwölf Monaten 81 Prozent der deutschen Unternehmen von Datendiebstahl, Industriespionage oder Sabotage betroffen. Der durch Cyberangriffe verursachte Gesamtschaden für die deutsche Wirtschaft wird auf rund 266 Milliarden Euro geschätzt. Besonders betroffen sind mittelständische Unternehmen, die komplexe IT-Landschaften betreiben und auf stabile Abläufe angewiesen sind, während Ressourcen und Zeit oft begrenzt sind. Die Frage lautet also nicht mehr, ob ein Angriff eintritt, sondern wann und wie gut ein Unternehmen darauf vorbereitet ist, den Betrieb unter Druck stabil zu halten.

2



Incident Response ist die operative Antwort auf diesen Moment. Der Umgang mit einem Cyberangriff entscheidet darüber, ob dieser kontrolliert bewältigt - oder zur Krise wird. In der Theorie ist der Ablauf klar: erkennen, eindämmen, analysieren, wiederherstellen. In der Praxis jedoch ist Incident Response ein vielschichtiger Prozess, der technisches Können, organisatorische Klarheit und kommunikative Disziplin vereint.

Viele Unternehmen unterschätzen diesen Aspekt. Sie erwarten schnelle Lösungen, eine Art digitale Feuerwehr, die kommt, Systeme säubert und alles wieder zum Laufen bringt. Doch Incident Response ist kein punktueller Eingriff, sondern ein strukturierter Krisenprozess mit klaren Rollen, definierten Phasen und vielen Abhängigkeiten.

Der entscheidende Faktor ist Zeit. **Jede Minute nach einem Angriff beeinflusst die Schadenshöhe, die Wiederherstellungsdauer und das Vertrauen von Kunden und Partnern**. Doch Zeitgewinn entsteht nicht in der Krise, sondern in der Vorbereitung. Wer vorher weiß, wer entscheidet, wie kommuniziert wird und welche Systeme kritisch sind, kann im Ernstfall ruhig und zielgerichtet reagieren.

Erfahrungen aus realen Einsätzen zeigen: Die technische Wiederherstellung ist nur ein Teil der Aufgabe. Ebenso wichtig ist der organisatorische Wiederaufbau - Prozesse, Verantwortlichkeiten und Vertrauen. Incident Response bedeutet nicht nur, Systeme wieder funktionsfähig zu machen, sondern Stabilität, Transparenz und Handlungsfähigkeit zurückzugewinnen.

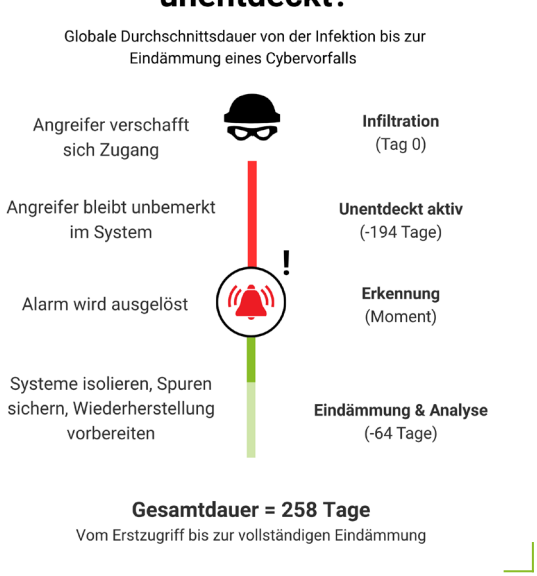
Quelle:

1. Bitkom Research 2024, n = 1.003 Unternehmen, S. 13.
2. Bitkom Research, Wirtschaftsschutz 2024, S. 14.

Vom Alarm zur Analyse

Der Moment, in dem ein Angriff entdeckt wird, ist selten spektakulär. Kein lauter Alarm, kein sofort sichtbarer Schaden. Oft ist es ein kleines Signal: eine verdächtige Anmeldung, ein ungewöhnlicher Datenfluss oder ein Mitarbeiter, der bemerkt, dass etwas nicht stimmt. Genau in diesem Moment entscheidet sich, ob ein Unternehmen vorbereitet ist.

1



Die ersten Stunden nach der Entdeckung eines Vorfalls sind entscheidend. Was dann geschieht, bestimmt den Verlauf der gesamten Reaktion. In der Theorie gilt: Systeme isolieren, Spuren sichern, Abläufe stabilisieren. In der Praxis heißt das, Prioritäten unter Unsicherheit zu setzen und Entscheidungen zu treffen, bevor alle Fakten vorliegen.

Ein häufiger Fehler: Systeme werden zu früh heruntergefahren oder neu gestartet, oft aus dem Reflex heraus, Schaden zu begrenzen. Doch solche Maßnahmen können Beweise vernichten. Forensische Spuren, die später zeigen, wie der Angriff erfolgte, gehen verloren.

Ebenso gefährlich ist das Gegenteil: das Zögern. Viele Vorfälle werden zu spät als Krise erkannt, weil Entscheidungswege unklar sind. Wer darf den Notfall ausrufen? Wer informiert externe Partner? Wer hat Zugriff auf Protokolle oder Backups? Fehlende Strukturen führen zu Verzögerungen und verschaffen Angreifern Zeit, weitere Systeme zu kompromittieren.

In einem professionellen Einsatz beginnt die Arbeit mit einer Bestandsaufnahme: Welche Systeme sind betroffen, welche Daten manipuliert oder exfiltriert, welche Abhängigkeiten bestehen zu anderen Anwendungen oder Standorten? Parallel werden Logdaten, Speicherabbilder und Konfigurationen gesichert.

Diese Phase verlangt mehr als Technik. Sie erfordert Ruhe, Erfahrung und das Verständnis, dass Beobachtung oft wertvoller ist als Aktion. Nicht jeder Alarm ist ein Angriff, nicht jede Auffälligkeit ein Vorfall. Doch wer zu früh handelt oder zu spät reagiert, riskiert Fehlentscheidungen.

Ein typisches Problem zeigt sich immer wieder: fehlendes Logmanagement. Viele Organisationen speichern Protokolle zu kurz oder verteilen sie auf mehrere Systeme, die nicht zentral ausgewertet werden können. Wenn ein Angriff erst nach Tagen bemerkt wird, fehlen oft entscheidende Daten, sodass die Analyse zur Spurensuche im Dunkeln wird.

Vom Alarm zur Analyse führt kein standardisierter Weg, doch erfolgreiche Einsätze folgen ähnlichen Mustern: Besonnenheit, Präzision und klare Kommunikation. In dieser Phase geht es nicht nur um Daten, sondern um Orientierung.

Quelle:

1. IBM Cost of a Data Breach Report 2024, bestätigt auch durch Varonis & IT Governance USA

Struktur statt Aktionismus

In den ersten Stunden nach einem Angriff ist die Versuchung groß, sofort zu handeln. Hauptsache, es passiert etwas: Systeme trennen, Passwörter ändern, Server neu starten.

Incident Response folgt einem klaren Ablauf, der im Idealfall schon vorher festgelegt und geübt wurde. Die Phasen sind bekannt: Erkennung, Eindämmung, Analyse, Wiederherstellung. Doch in der Praxis verschwimmen sie oft. Zu viel Aktionismus führt dazu, dass Maßnahmen sich überlagern, Informationen verloren gehen und Verantwortlichkeiten unklar werden.

Ein geordneter Prozess beginnt mit der Bewertung der Lage: Was ist passiert, wie weit reicht der Schaden, welche Systeme sind kritisch? Diese Einschätzung ist die Basis für alle weiteren Schritte. Erst dann folgt die Eindämmung, also das Stoppen der Ausbreitung, bevor weitere Bereiche betroffen sind.

In der Praxis haben sich fünf Kernprinzipien bewährt:

1. Klare Verantwortlichkeiten und schnelle Entscheidungen
2. Saubere Dokumentation jedes Schritts
3. Priorisierung der Systeme nach Kritikalität
4. Laufende Kommunikation zwischen Technik, Management und Partnern
5. Überprüfung und Nachjustierung aller Maßnahmen

Parallel dazu läuft die Kommunikation. Das Incident-Response-Team informiert Management, IT und Partner. Alle müssen wissen, was geschieht, aber ohne Panik. Struktur ersetzt Hektik. Sie schafft Orientierung und Vertrauen.

Jede Maßnahme wird dokumentiert, jede Entscheidung begründet. Denn ein Incident ist keine einzelne Handlung, sondern eine Kette von Entscheidungen unter Druck.

Am Ende gilt: Geschwindigkeit ist wichtig, aber ohne Struktur riskant. Ein Plan entfaltet seine Wirkung nur, wenn er vorher verstanden und eingeübt wurde. Wer ihn erst in der Krise zur Hand nimmt, verfügt zwar über ein Dokument, aber nicht über die Orientierung, die in diesem Moment notwendig ist.


PODCAST
CYBER SECURITY
Basement
In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.
Jetzt reinhören
Spotify
Apple Podcast
YouTube Music
amazon music
und noch mehr...

Kommunikation in der Krise

Ein Sicherheitsvorfall ist immer auch eine Kommunikationskrise. Selbst die beste Technik verliert ihre Wirkung, wenn Informationen unvollständig sind oder Entscheidungen nicht abgestimmt erfolgen.

Kommunikation muss präzise, aber kontrolliert erfolgen. Nicht jedes Detail muss sofort geteilt werden, doch alle relevanten Akteure müssen über die gleiche Lageeinschätzung verfügen.

Das technische Team liefert Fakten, das Management entscheidet, die Kommunikation hält den Überblick und sorgt für Einheitlichkeit. Wer zu früh zu viel sagt, riskiert Verwirrung. Wer zu spät reagiert, verliert Glaubwürdigkeit.

Auch externe Partner - Versicherer, Behörden, Kunden - müssen mit Bedacht eingebunden werden. Ein falsches Wort kann rechtliche oder operative Folgen haben. Transparenz ist kein Risiko, sondern ein Werkzeug: Wer offen und abgestimmt kommuniziert, behält die Kontrolle über die Erzählung des Vorfalls.

> „Eine Krise zeigt, ob ein Unternehmen kommunizieren kann. Nicht, ob es redet, sondern ob es versteht, was gesagt werden muss Und wann besser geschwiegen wird."
>
> **– Andreas Papadaniil, CEO, suresecure**

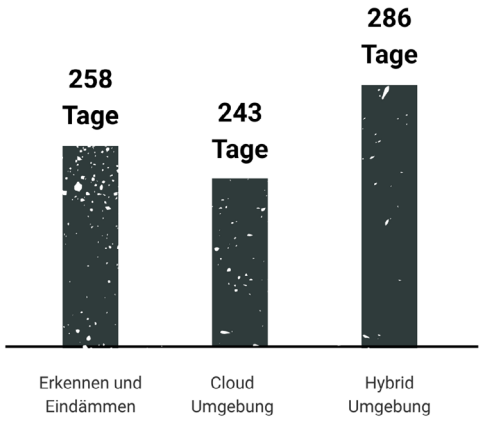
Eine Krise wird selten durch Technik bewältigt, sondern durch klare Köpfe, geübte Abläufe und saubere Kommunikation. Sie schafft Orientierung, wo Unsicherheit herrscht, und verhindert so, dass aus einem Vorfall ein Vertrauensverlust entsteht.

Recovery ist ein stiller Kraftakt.

Wenn der Angriff gestoppt ist, kehrt kurz Ruhe ein. Systeme laufen wieder, der Schaden scheint begrenzt. Doch was wie das Ende aussieht, ist in Wahrheit der Beginn der anspruchsvollsten Phase: der Wiederherstellung.

Recovery bedeutet, Systeme, Prozesse und Vertrauen Schritt für Schritt neu aufzubauen. Dabei gilt: Zuerst die kritischen Systeme wie Produktion, Kommunikation und Kundenzugänge, danach der Rest. Der sogenannte Notbetrieb ist oft nach ein bis zwei Wochen erreicht, doch bis alles stabil läuft, vergehen meist mehrere Wochen oder sogar Monate.

Wie lange dauert Incident Response weltweit?



Parallel läuft die organisatorische Aufarbeitung: forensische Analysen, Berichte an Behörden und Versicherungen, Dokumentation der Erkenntnisse. Es ist die Phase, in der Präzision wichtiger ist als Tempo. Wer jetzt unkoordiniert handelt, riskiert neue Schwachstellen.

Wichtige Aufgaben in der Recovery-Phase sind:

1. Wiederherstellung zentraler Systeme und Kommunikationsdienste
2. Validierung der Integrität aller Komponenten
3. Überprüfung von Backups und Sicherheitskonfigurationen
4. Abschluss forensischer Analysen und Berichterstattung

Prüfung und Anpassung von Prozessen und Verantwortlichkeiten Recovery ist mehr als Technik. Sie ist ein Test für Organisation und Führung: Wie konsequent bleiben Prioritäten, wenn der Druck wächst? Wie gut greifen Prozesse, wenn Routinen versagen?

Am Ende zählt nicht, wann die Systeme wieder laufen, sondern wann Vertrauen und Kontrolle zurückkehren: technisch, organisatorisch und menschlich.

Quelle:

1. IBM Cost of a Data Breach 2024 – cdn.table.media/ibm-cyber-report2024.pdf

Vorbereitung als Schlüssel

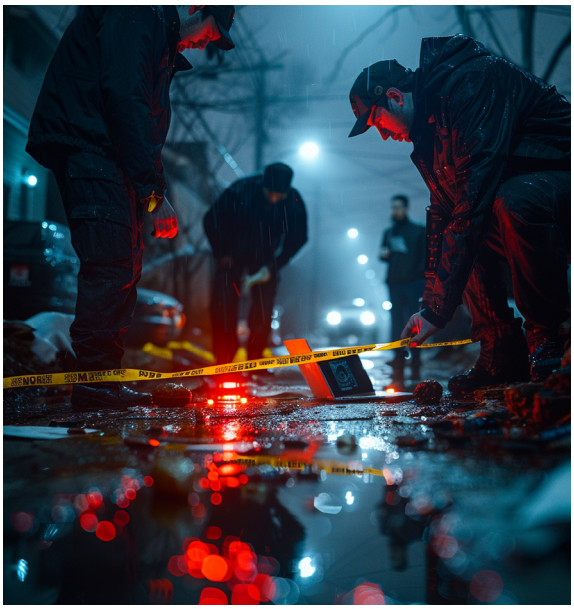
Jede Incident Response beginnt lange vor dem ersten Angriff. Ob ein Unternehmen in der Krise handlungsfähig bleibt, entscheidet sich in Zeiten der Ruhe.

Ein starkes Konzept beruht auf drei Säulen: Struktur, Verantwortung und Übung. Struktur bedeutet klare Rollen, Eskalationsstufen und Kommunikationswege. Verantwortung bedeutet, dass Incident Response Chefsache ist, keine IT-Routine. Übung bedeutet, Abläufe so oft zu trainieren, bis sie selbstverständlich funktionieren.

Tabletop-Übungen sind das beste Mittel, um Schwachstellen sichtbar zu machen. Sie zeigen, ob Teams zusammenarbeiten, ob Kommunikation funktioniert und Entscheidungen zur richtigen Zeit getroffen werden. Jede vorbereitete Stunde spart in der Krise ein Vielfaches an Zeit und Kosten.

Ein Incident-Response-Retainer mit externen Partnern sichert zusätzlich Handlungsspielraum. Wer im Ernstfall auf bekannte Strukturen und vertraute Ansprechpartner zurückgreifen kann, gewinnt wertvolle Zeit und verhindert Fehler.

> „Vorbereitung ist kein Projekt, sondern ein Zustand. Sie wächst mit jeder Überprüfung, jeder Übung und jeder bewussten Entscheidung, Verantwortung zu übernehmen."
>
> **– André Ditzel, Senior IR-Analyst, suresecure**



Nach dem Angriff: Lernen statt vergessen

Wenn der Betrieb wieder stabil ist, beginnt die wichtigste Phase: das Lernen. Die Nachbereitung entscheidet, ob ein Angriff einmalig bleibt oder sich wiederholt.

Sie besteht aus drei Schritten: Analyse, Bewertung und Umsetzung. Die Nachbereitung sollte interdisziplinär erfolgen. Das Ziel ist nicht Schuldzuweisung, sondern Verbesserung. Sie zeigt, wie Technik, Organisation und Kommunikation zusammenwirken. Oder wo sie versagen.

Ein Post-Incident-Report fasst alle Erkenntnisse zusammen und dokumentiert, was künftig anders laufen wird. Er ist kein Pflichtdokument, sondern ein Werkzeug zur Weiterentwicklung.

Unternehmen, die offen analysieren und konsequent lernen, entwickeln echte Widerstandsfähigkeit. Nach einem Angriff zeigt sich ihre Reife: Nicht wer unverwundbar ist, sondern wer lernfähig bleibt, ist resilient.

Fazit:
Kontrolle im Chaos

Ein Sicherheitsvorfall ist heute kein Ausnahmezustand mehr, sondern Teil der digitalen Realität. Grundsätzlich kann jedes Unternehmen betroffen sein, unabhängig von Branche, Größe oder Reifegrad. Entscheidend ist nicht, ob ein Angriff passiert, sondern wie darauf reagiert wird.

Incident Response verbindet Technik, Organisation und Kommunikation. Sie ist kein Projekt, sondern eine Haltung: die Fähigkeit, Kontrolle zu behalten, wenn sie zu entgleiten droht. Wer vorbereitet ist, gewinnt Zeit. Wer strukturiert reagiert, behält Orientierung. Und wer aus Vorfällen lernt, wird mit jeder Krise widerstandsfähiger.

In jedem Angriff steckt auch die Chance, sich zu verbessern. Resilienz entsteht, wenn Wissen, Erfahrung und Verantwortung zusammenwirken - nicht im Ausnahmezustand, sondern im Alltag.

Am Ende zeigt sich Stärke nicht darin, unverwundbar zu sein, sondern handlungsfähig zu bleiben, wenn alles auf dem Spiel steht.

Wie das Security Operations Center Unternehmen in jeder Phase unterstützt

Vor dem Angriff:

- Incident Response Management Plan (IRMP).
- Struktur, Rollen und Kommunikationswege klar definiert.
- Quickguide, RACI-Matrix und Wiederherstellungsplan schaffen Sicherheit im Ernstfall.

Während des Angriffs:
SafeGuard-Servicevertrag

- Innerhalb von zwei Stunden aktiv: ein erfahrenes Einsatzteam unter Leitung eines 24/7 verfügbaren Managers.
- Koordiniert, schnell, verlässlich.

Nach dem Angriff:
Notfallhilfe

- Fünf Phasen: Identifikation, Isolation, Bereinigung, Wiederherstellung, Analyse.
- Sorgt für Stabilität und verhindert erneute Kompromittierungen.

Weitere Informationen zum Thema:

Podcast-Folge:

Was leistet Incident Response wirklich?
Die Realität hinter dem Kriseneinsatz.

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de