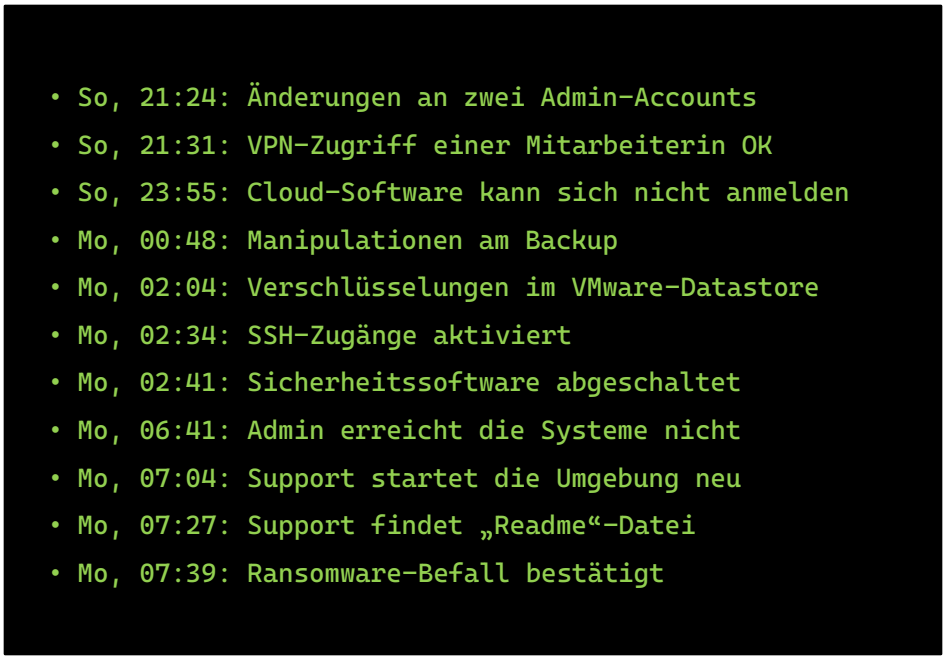

IT- & DigitalisierungsTag 2025
Region 38
29.10.2025
an der WelfenAkademie
IT & Digitalisierung
RATGEBER FÜR UNTERNEHMEN
SERVICESEITEN
KÜNSTLICHE INTELLIGENZ
SECURITY
IT & Cyber
eRECHNUNGEN
Dokumentenmanagement
mediaworld

*Bild: Unsplash.com, Jonathan Borba*

Ein Anruf auf der Mailbox:

> *Hi André, hier ist Michael.*
> *Kannst du mich mal dringend zurückrufen? Hier passiert grad irgendwas Komisches. Ich komm nicht auf unsere Systeme.*

- Fallbeispiel aus diesem Jahr (2025)
  - High-Tech-Unternehmen, weltweit tätig, 500-1000 Mitarbeiter:innen
  - Vorfall aus dem Februar 2025
  - Notbetrieb in der ersten Woche
  - Übergangsbetrieb nach einem Monat
  - Oktober 2025: Immer noch im Recovery
- Was ist da passiert?




Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


Nils Kaczenski
*ATD | Systemhaus, Chief Technology Officer*
*Microsoft MVP Enterprise & Platform Security*

N.Kaczenski@atd.de

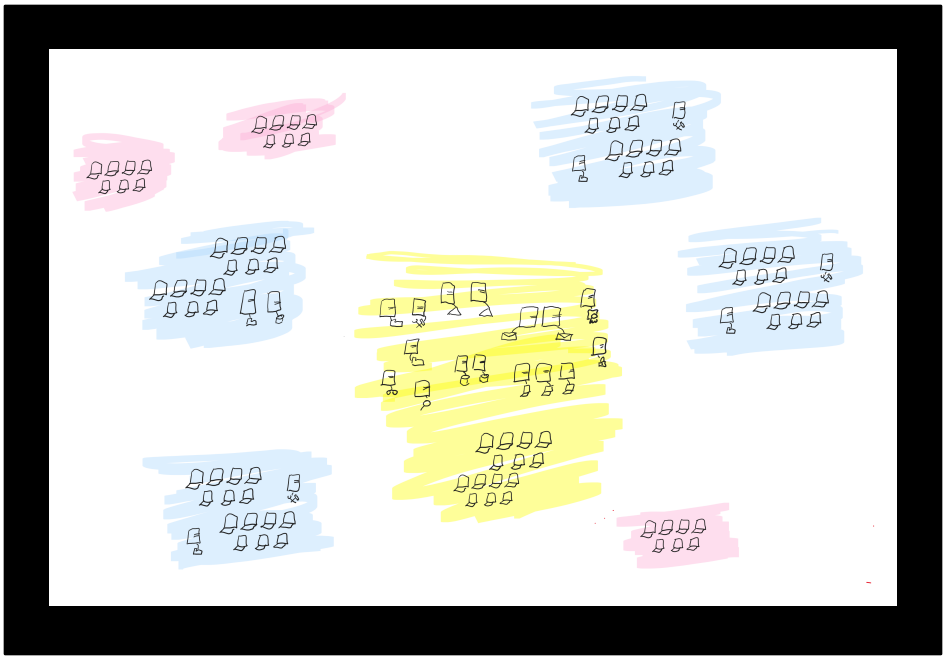

ATD ist ein führendes IT-Beratungshaus aus Braunschweig mit den Schwerpunkten

- IT Security
- IT Service
- IT-Strategien

Als IT-Dienstleister sind wir seit 30 Jahren am Markt, an mittlerweile 6 Standorten und mit 120 Mitarbeiter:innen in Norddeutschland. Unsere Kunden sind mittelständische Unternehmen aus dem gesamten deutschsprachigen Raum.

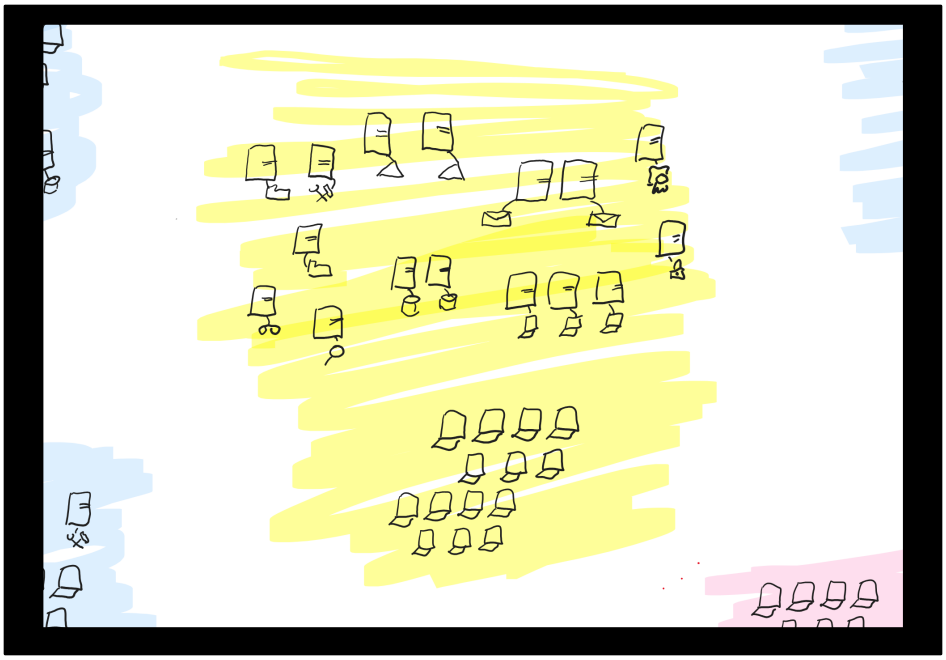
Wir verbinden Beratungskompetenz mit Expertise zur praktischen Umsetzung – in der IT-Security heißt das: ATD betreut Sie in der operativen Sicherheit im Tagesgeschäft und entwickelt mit Ihnen die Sicherheitsstrategie, die zu Ihrem Unternehmen passt.


Wie funktioniert heute eigentlich ein Hackerangriff?

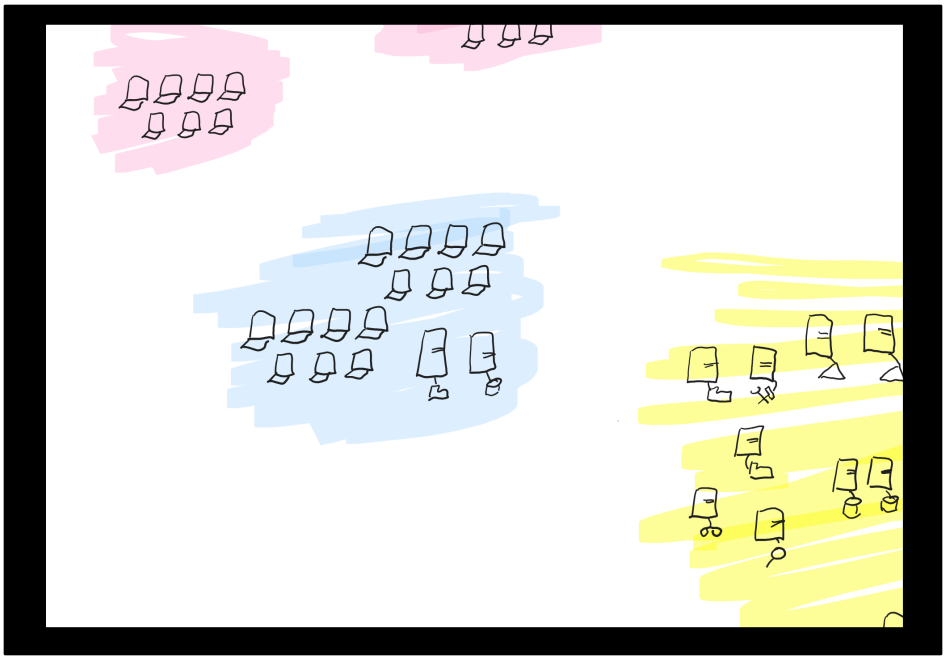


IT-Netzwerke sind auch in mittelständischen Unternehmen erstaunlich komplex. Auch wer seine IT gut im Griff hat, steht unter dem Risiko, dass einzelne Bereiche Schwachstellen aufweisen.

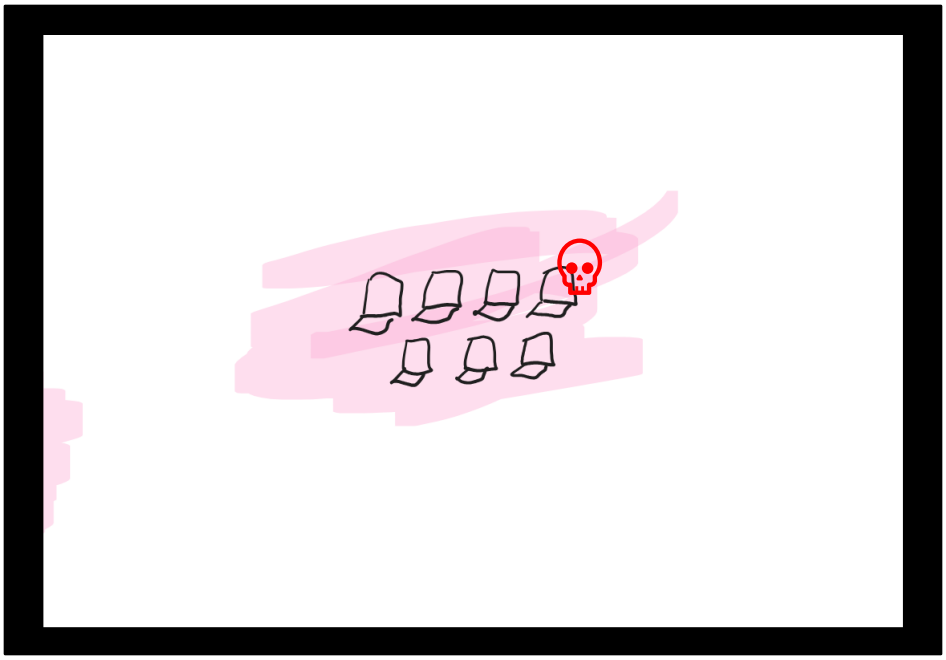
Ein „typisches“ mittelständisches Unternehmen betreibt oft mehrere IT-Standorte mit verteilten Systemen.



In der Zentrale eines Netzwerks befinden sich meist die wichtigen Anwendungen, Dienste und Daten. Dort ist üblicherweise auch der größte Teil des IT-Teams.

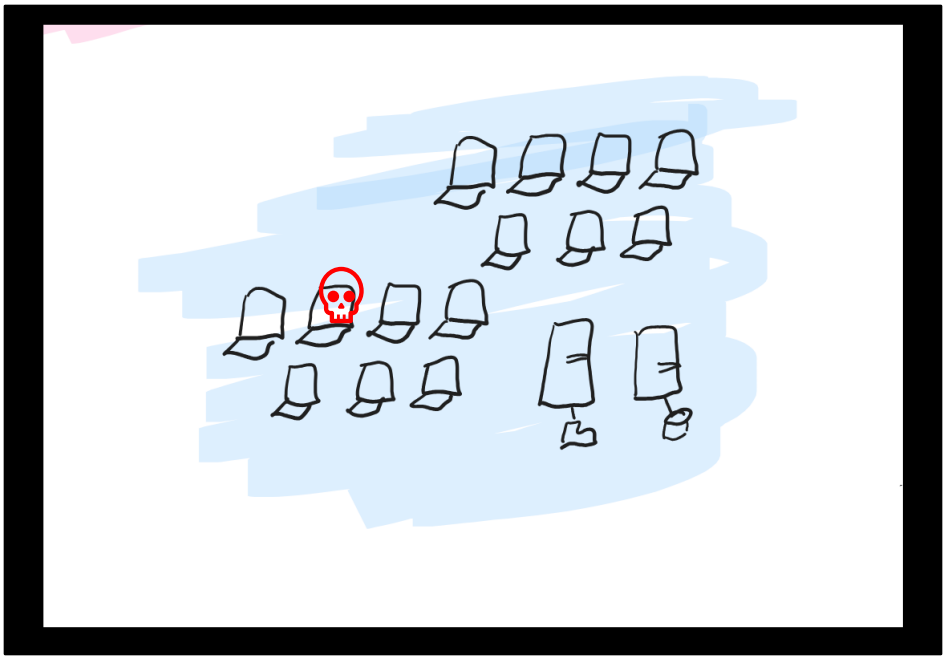


Außenstellen und kleinere Standorte haben meist nur die nötigen Daten und Dienste vor Ort. Die Anbindung ist über Firewalls und VPN-Techniken gesichert.

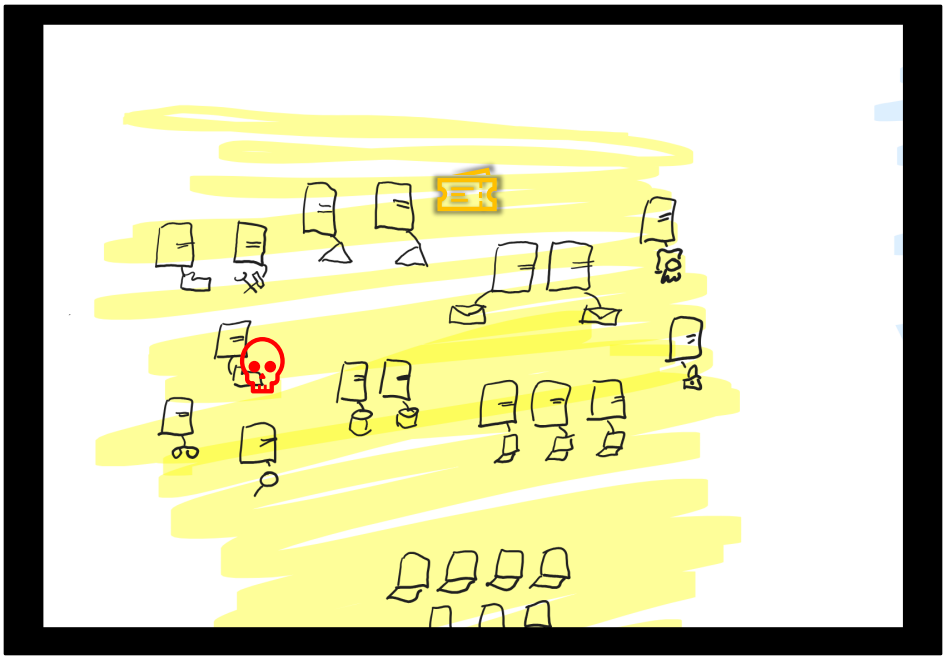


Doch gerade an den „Rändern“ des Netzwerks gibt es oft übersehene Schwachstellen. Das könnten Rechner sein, die noch nicht auf dem aktuellen Update-Stand sind.

Manchmal ist es aber auch ganz anders: Die Mail eines Geschäftspartners enthält ein Dokument, das völlig plausibel ist. Schnell geöffnet, um es zu prüfen – und schon infiziert der Virus den Rechner.



Eine aktive Malware verbreitet sich von PC zu PC. Das ist oft viel zu leicht, wenn etwa der Admin-Zugang auf allen Rechnern derselbe ist.
So wandert der Virus von Rechner zu Rechner. IT-Sicherheitsexperten sprechen hier von „Lateral Movement“.

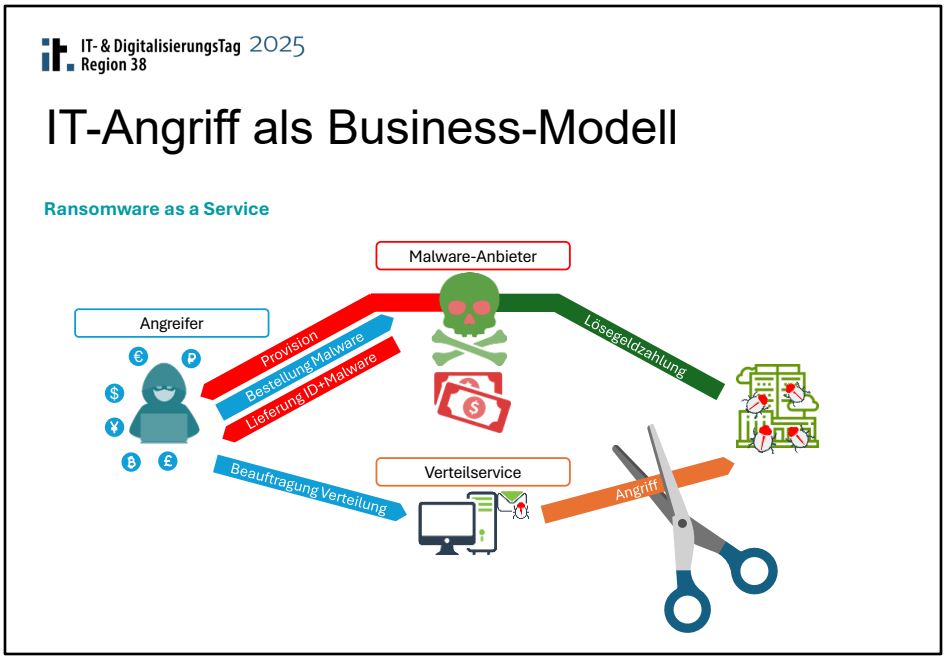


Meist findet die Malware dann Angriffspunkte, um mehr Zugriffsrechte zu erhalten („Privilege Escalation“). So dauert es nicht lang, und der Angreifer hat Adminrechte nicht nur auf einem PC, sondern sogar auf einem Server. Es ist dann nur eine Frage der Zeit, bis die Malware auch die Server übernimmt, die den Admin-Zugang zum ganzen Netz kontrollieren. Das Netzwerk ist endgültig in der Gewalt der Angreifer.

Um auch Reinigungsversuche zu überdauern, stellen sich Angreifer „Golden Tickets“ aus, die es später ermöglichen sollen, erneut einzubrechen.


*Bild: Unsplash.com, Andrew Winkler*

- Verhalten des Kunden nach dem Incident
  - Shutdown
  - Große Ratlosigkeit
  - Verbale Bereitschaft, ab nun alles besser zu machen




Moderne Hackerbanden arbeiten nach denselben modernen Prinzipien wie die offizielle Wirtschaft: Sie sind hoch arbeitsteilig organisiert und bieten ihre Techniken als Dienstleistung an. Die Bezeichnung „Ransomware as a service“ ist keine Ironie, sondern eine zutreffende Beschreibung.

Als einzelnes Unternehmen kann man nur an einer Stelle ansetzen und die tatsächlichen Angriffe verhindern (besser: unwahrscheinlich machen) oder so schnell wie möglich beenden.


Was hilft in solchen Situationen?
Was hat dem realen Kunden aus unserer Praxis-Fallgeschichte geholfen?


*Bild: Unsplash.com, Immo Wegmann*

Da moderne Angriffe primär mit Datenverlusten arbeiten, die sie dem Opfer zufügen oder androhen, ist das primäre Gegenmittel eine leistungsfähige Datensicherung. Wichtig ist dabei, dass das Backup nicht zu simpel ist, denn Angreifer versuchen mittlerweile als erstes, die erreichbaren Datensicherungen zu zerstören, bevor sie den eigentlichen Angriff beginnen.


*Bild: Unsplash.com, Michel E*

Die Datensicherung ist die Vorsorge. Im Moment eines Angriffs – oder sobald dieser bemerkt wird – kommt es auf eine kompetente Erstreaktion an. Es gibt dabei zwei Ziele:

1. die Auswirkungen des Angriffs begrenzen
2. den Angriff beenden

Die allerersten Reaktionen sollte jedes Unternehmen selbst einüben. So schnell wie möglich braucht es dann erfahrene Unterstützung. Meist beauftragt man hierzu Dienstleister für Incident Response.

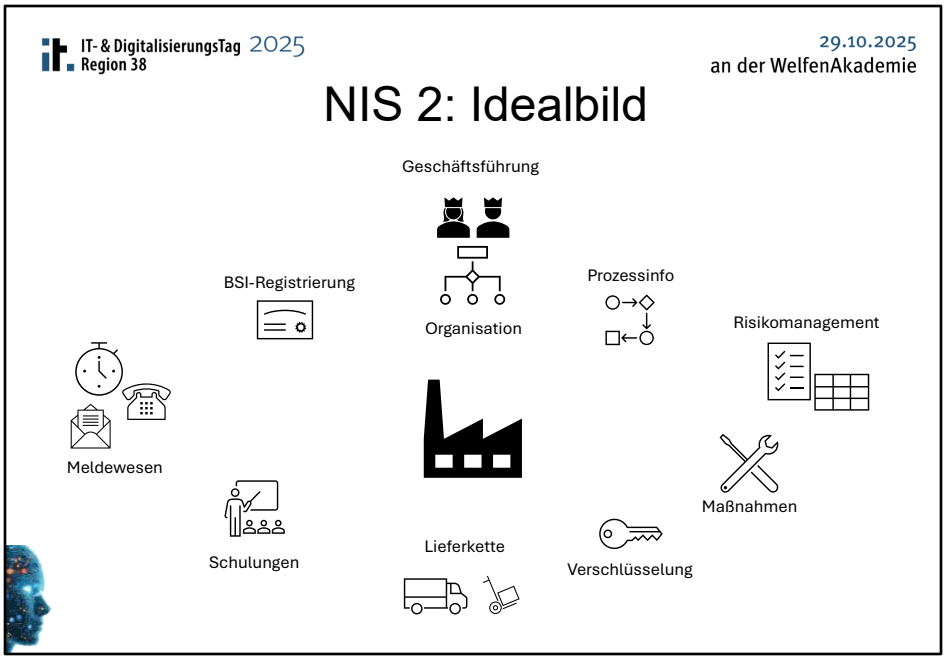

*Bild: Unsplash.com, ThisIsEngineering*

Die Krisenreaktion (Incident Response) läuft meist parallel zu Aktivitäten, die den Geschäftsbetrieb wiederherstellen. In den meisten Fällen ist in dieser Zeit noch lange nicht an „normales Business“ zu denken, sondern es geht um Notbetrieb. Koordiniertes Handeln mit erfahrener Unterstützung ist wichtig, um Chaos zu vermeiden.


*Bild: Unsplash.com, Immo Wegmann*

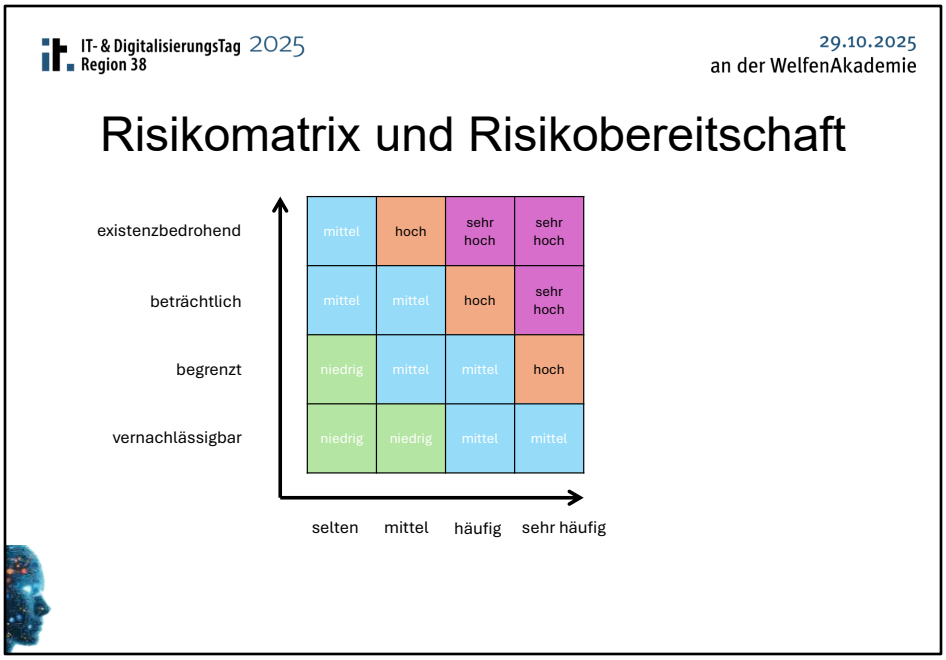
Wenn ich oben behauptet habe, dass Backup am wichtigsten sei, dann war das nicht richtig. Es kommt nicht aufs Backup an, sondern auf das Recovery. Das ist kein Wortspiel, sondern ein Unterschied ums Ganze.


Wie hilft Compliance in der IT-Security?
Ist das überhaupt Sicherheit – oder nur lästiger Papierkram?




Was wir als „Compliance“ bezeichnen, ist vor allem eine Denkweise, die sich in verschiedenen Regelwerken und Normen niederschlägt. Während Normen und Regeln ost lästig und umständlich erscheinen, ist die Denkweise höchst nützlich. Denn sie schafft eine Orientierung, um Sicherheit in der Organisation und der gesamten Technik-Landschaft zu verankern.

Das aktuellste Beispiel hierfür ist die Europa-Richtline NIS 2. Sie beruht auf denselben Konzepten wie Industrie-Regelwerke (TISAX, ISO 27001 usw.) und fordert einen systemarischen Umgang mit Informationssicherheit. Sie betrifft einen Großteil der mittelständischen Wirtschaft in Europa.



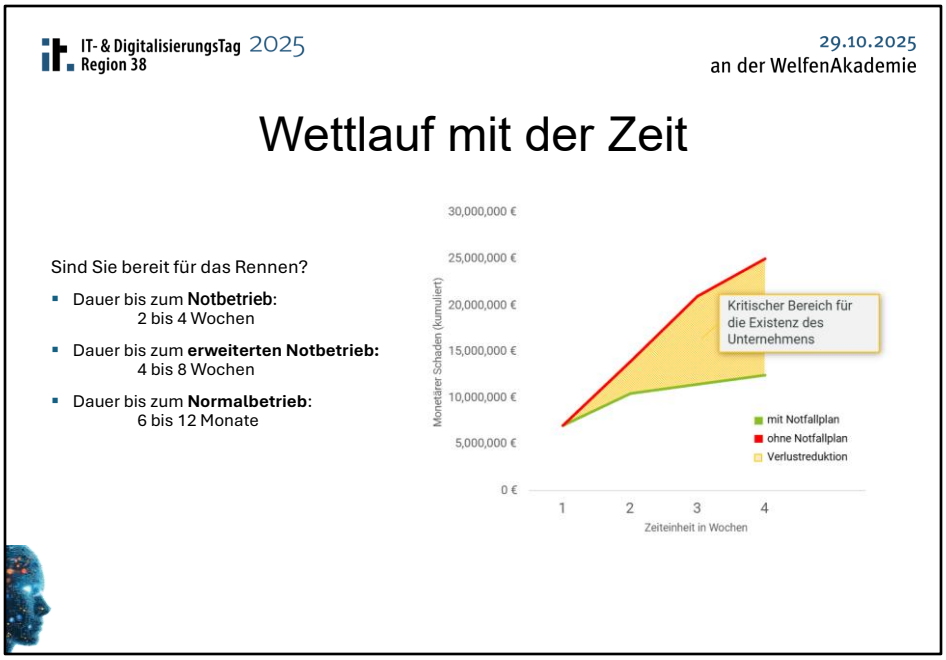

Im Mittelpunkt der NIS-2, von TISAX oder der ISO 27001 steht ein professionelles Risikomanagement. Hiervon sieht man oft nur formale Tabellen. Dahinter steht aber ein organisatorisches Gerüst, das Unternehmen erst in die Lage versetzt, auf Risiken und Angriffe zu reagieren.

Risiken sind Angriffe, die noch nicht begonnen haben.


*Bild: Unsplash.com, Tachina Lee*

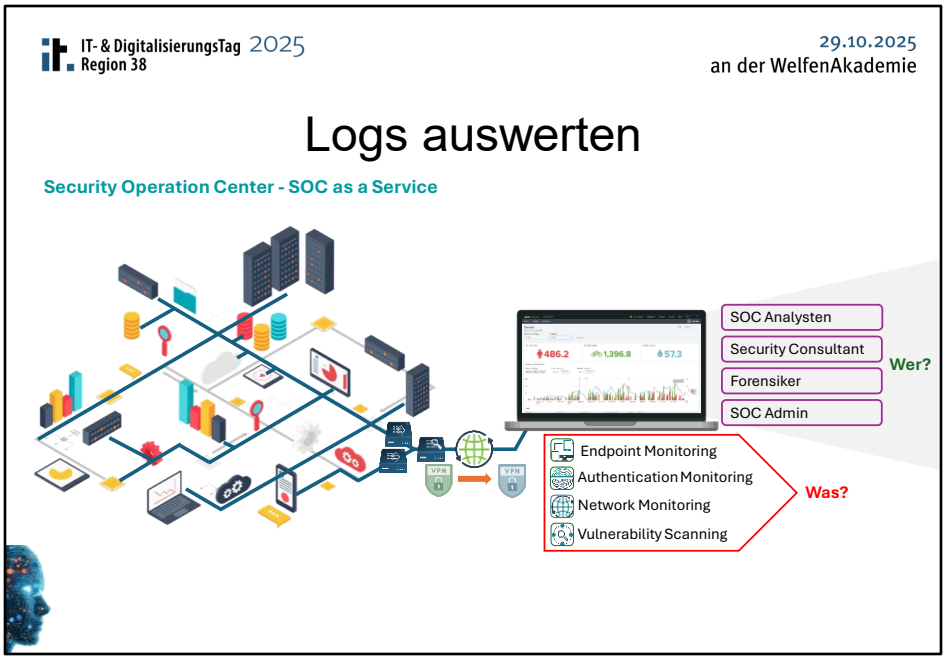
Compliance ist weit mehr als Regularien. Sie bildet die Grundlage, um Maßnahmen abzuwägen.


IT-Sicherheit kann man nicht ignorieren.
Man muss sie aber nicht vollständig selbst machen.




Technische und organisatorische IT-Sicherheit können Schäden nicht vollständig verhindern. Sie können sie aber weniger wahrscheinlich machen.

Und die Vorbereitung kann die Zeit verkürzen, die ein Unternehmen im Schadensfall braucht, um ihr Geschäft wieder aufzunehmen.




Viele technische Maßnahmen der IT-Sicherheit beruhen darauf, Informationen zu sammeln. Diese Informationen können sehr nützlich sein, um einen Schaden zu beheben oder einen Angriff zu verstehen und abzuwehren.

Die systematische Sammlung und Auswertung von Informationen zur IT-Sicherheit geschieht heute oft über ein Security Operations Center (SOC). Konzerne betreiben solche SOCs oft selbst. Für den Mittelstand sind SOC-Dienstleister eine gute Alternative: SOC as a Service.


Bild: Unsplash.com, Kevin Charit

SOCs haben mehere Evolutionsstufen durchlaufen. Grob lassen sich unterscheiden:

- SOC 1.0: systematische, aber nur teilweise automatisierte Sammlung und Auswertung von Informationen (SIEM, Security Information and Event Management), meist reaktiv ausgerichtet
- SOC 2.0: standardisierte, hochautomatisierte Sammlung und Auswertung von Informationen. Die Automatisierung ermöglicht auch teils automatisierte Reaktionen und kann Angriffe manchmal früh unterbrechen oder sogar verhindern (aktiv statt reaktiv)
- SOC 3.0: Sammlung und Auswertung mit KI-Unterstützung. Automatisierte Erkennung von Anomalien oder Angriffsmustern ermöglicht früheres Reagieren, idealerweise unterbinden die Automatismen Angriffe noch im Entstehen („proaktiv“)


IT-Security ist weit mehr als nur Technik und Regelwerks-Compliance. Ein Managed-Security-Prozess kann gemeinsam zwischen einem Unternehmen (Fachebene) und einem erfahrenen Dienstleister (IT-Ebene) entworfen und umgesetzt werden.

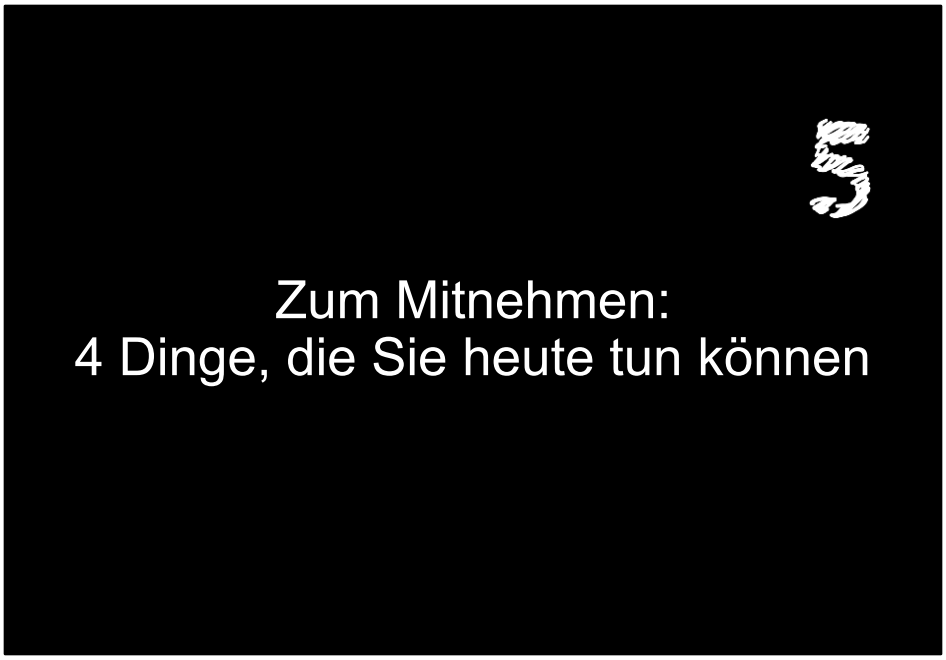
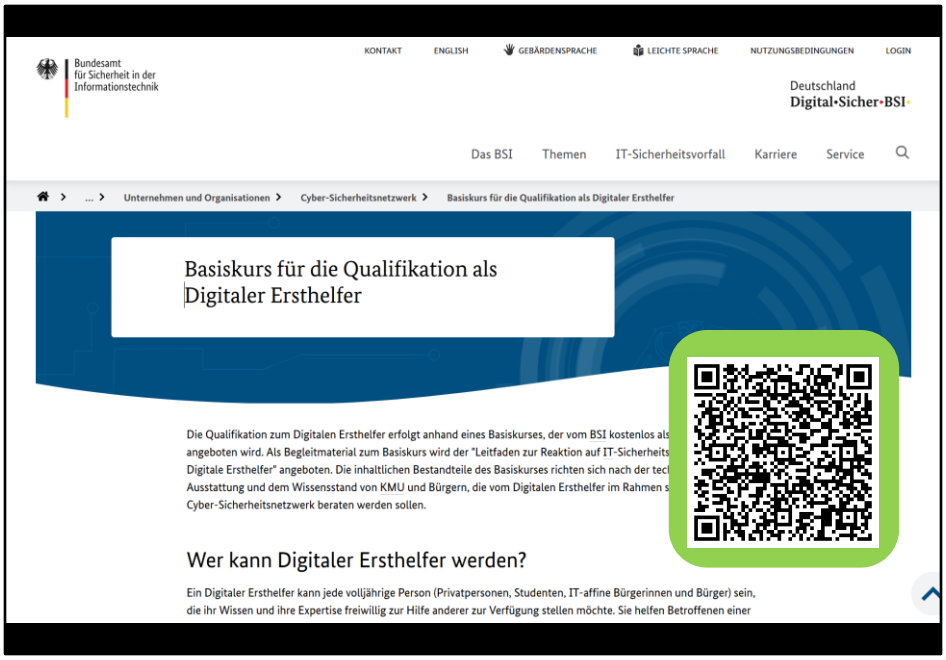

Zum Mitnehmen:
4 Dinge, die Sie heute tun können

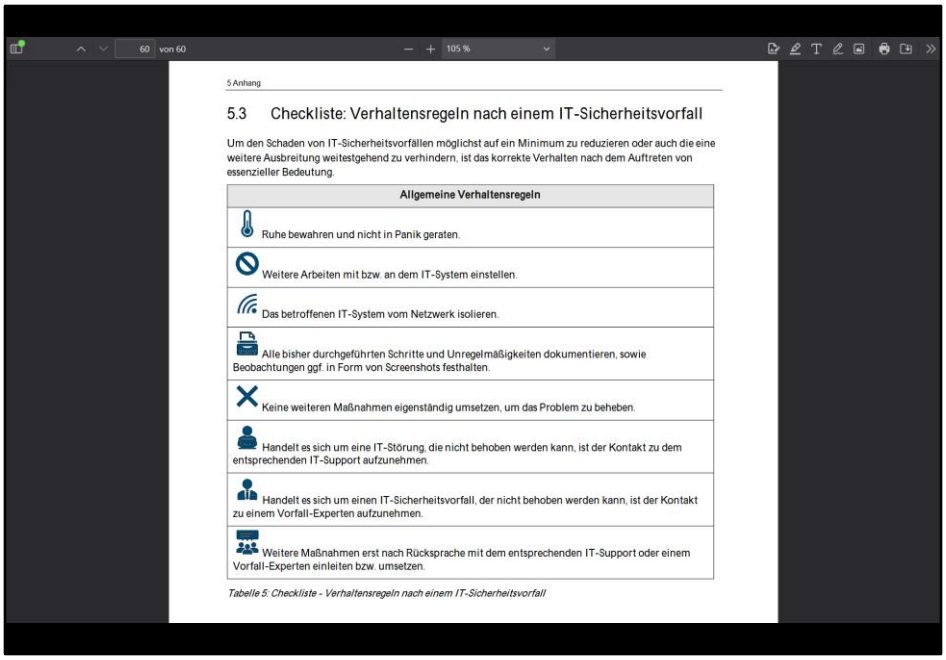

*Bild: Unsplash.com, Chris Linnett*

Vier Sofortmaßnahmen:

1. Prüfen Sie noch heute ihr Backup. Enthält es alles Wichtige?
   *Ergänzen Sie dies durch regelmäßige konzeptionelle Prüfungen. Aber gehen Sie den ersten Schritt noch heute an.*
2. Prüfen Sie Ihren Malware-Schutz.
   *Auch hier ergänzen Sie den Ad-hoc-Check um regelmäßige konzeptionelle Reviews.*
3. Kein Shutdown nach einem Angriff.
   *Weisen Sie Ihre IT-Mitarbeiter:innen und Ihr Personal darauf hin, dass „Abschalten" im Fall eines Falles nur die zweitbeste Option ist. Das Abschalten kann Beweise vernichten. Die bessere Variante: Systeme vom Netz trennen (LAN-Kabel ziehen, WLAN und Mobilfunk abstellen).*
4. Bilden Sie Digitale Ersthelfer aus.
   *Externe Kosten: Null. Interne Kosten: ein paar Stunden. Wie das geht, steht auf den folgenden Seiten.*




https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Digitaler_Ersthelfer/Onlinekurs/Onlinekurs_node.html



5 Anhang

## 5.3 Checkliste: Verhaltensregeln nach einem IT-Sicherheitsvorfall

Um den Schaden von IT-Sicherheitsvorfällen möglichst auf ein Minimum zu reduzieren oder auch die eine weitere Ausbreitung weitestgehend zu verhindern, ist das korrekte Verhalten nach dem Auftreten von essenzieller Bedeutung.

| Allgemeine Verhaltensregeln |
| --- |
| Ruhe bewahren und nicht in Panik geraten. |
| Weitere Arbeiten mit bzw. an dem IT-System einstellen. |
| Das betroffenen IT-System vom Netzwerk isolieren. |
| Alle bisher durchgeführten Schritte und Unregelmäßigkeiten dokumentieren, sowie Beobachtungen ggf. in Form von Screenshots festhalten. |
| Keine weiteren Maßnahmen eigenständig umsetzen, um das Problem zu beheben. |
| Handelt es sich um eine IT-Störung, die nicht behoben werden kann, ist der Kontakt zu dem entsprechenden IT-Support aufzunehmen. |
| Handelt es sich um einen IT-Sicherheitsvorfall, der nicht behoben werden kann, ist der Kontakt zu einem Vorfall-Experten aufzunehmen. |
| Weitere Maßnahmen erst nach Rücksprache mit dem entsprechenden IT-Support oder einem Vorfall-Experten einleiten bzw. umsetzen. |

*Tabelle 5: Checkliste - Verhaltensregeln nach einem IT-Sicherheitsvorfall*

Aus den Unterlagen für die Digitalen Ersthelfer (BSI).


IT- & DigitalisierungsTag 2025
Region 38
29.10.2025
an der WelfenAkademie
Alle Beiträge des
IT- & DigitalisierungsTages
finden Sie online unter
www.it-tag-38.de
zum Download.
IT & Digitalisierung
RATGEBER FÜR UNTERNEHMEN
SERVICESEITEN
KÜNSTLICHE INTELLIGENZ
SECURITY
IT & Cyber
eRECHNUNGEN
Dokumentenmanagement
mediaworld