bitkom

Sicherheitskooperation Cybercrime

Cybersicherheit aktiv gestalten – ein Überblick für KMU und Behörden

Auf einen Blick

Cyberlage und daraus zu treffende Ableitungen für Unternehmen und Behörden

Ausgangslage

Die digitale Sicherheit ist ein entscheidender Faktor für den Wirtschaftsstandort Deutschland. Dabei stehen insbesondere kleine und mittelständische Unternehmen (KMU) und viele regionale Behörden bei der Thematik vor großen Herausforderungen. Hier gilt es einen Überblick zu möglichen Schutzmaßnahmen zu geben, um individuelle Handlungsoptionen ableiten zu können.

Allein 2022 gab es laut Bundeskriminalamt über 130.000 gemeldete Vorfälle im Bereich Cybercrime, Tendenz steigend. Als Cybercrime werden **alle Straftaten bezeichnet, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden.** Dazu zählen im engeren Sinne Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten. Im erweiterten Sinne Straftaten, die mittels Informationstechnik begangen werden, aber auch in der analogen Welt stattfinden könnten.

Der Digitalverband Bitkom untersucht zusammen mit dem Bundesamt für Verfassungsschutz seit 2015 jährlich, wie es um die deutsche Wirtschaft beim Thema Wirtschaftsschutz bestellt ist. Allein 2023 entstand der deutschen Wirtschaft durch Angriffe ein Schaden von fast 206 Milliarden Euro. Etwa 72 Prozent des Schadens (148 Mrd. Euro) entfallen dabei auf Cyberattacken.

Die Ergebnisse der aktuellen Studie 2023 unterstreichen, dass in Zeiten der zunehmenden Vernetzung all unserer Lebensbereiche die Resilienz der deutschen Wirtschaft gegen die steigenden Gefahren aus dem Cyberraum weiter ausgebaut werden muss. Es gilt, einen ganzheitlichen und nachhaltigen Wirtschaftsschutz zu etablieren. Dabei muss stets ein enger und vertrauensvoller Erfahrungsaustausch mit den Sicherheitsbehörden aufrechterhalten werden. Bitkom agiert dazu in der Sicherheitskooperation Cybercrime mit den Landeskriminalämtern Nordrhein-Westfalen, Hessen, Rheinland-Pfalz, Niedersachsen, Sachsen und Baden-Württemberg sowie mit weiteren staatlichen Partnern wie dem Bundeskriminalamt oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Cyberagentur des Bundes etc., um mit Awareness-Maßnahmen präventiv die IT-Sicherheit in Unternehmen und Behörden zu verbessern.

Bitkom-Bewertung

Grundsätzlich kann jedes Unternehmen und jede Behörde Opfer eines Cyberangriffs werden. Das größte Risiko für Unternehmen ist dabei die drohende Insolvenz. Für

Behörden steht deren Reputation und damit das Vertrauen der Bürgerinnen und Bürger in die freiheitlich-demokratische Grundordnung auf dem Spiel. Cybersicherheit ist eine vitale Aufgabe für jede Organisation, als Teil eines gesellschaftlichen Gesamtsystems.

Die Täterinnen und Täter agieren im höchsten Maße professionell, wobei 61 Prozent dem Bereich der organisierten Kriminalität zuzuordnen sind. Die kriminellen Strukturen agieren arbeitsteilig, im Sinne des Ansatzes: Cybercrime-as-a-Service.

Weitere Akteure liegen mit etwa sieben Prozent im Bereich ausländischer Nachrichtendienste, die es u. a. auf Know-how, Informationen über Zusammenhänge etc. oder die Sabotage von Infrastrukturen abgesehen haben. Auch andere Unternehmen oder Innentäter können Ausgangspunkt von Cybercrime sein.[1]

Dieser komplexen Gemengelage können wir nur mit einem integrierten Ansatz eines gemeinsamen Ökosystems aus Staat, Wirtschaft und Wissenschaft begegnen.

Das Wichtigste

- Unternehmen und Behörden sind Cybercrime nicht schutzlos ausgeliefert. Grundsätzlich sind Angriffsszenarien und mögliche Verteidigungsmöglichkeiten bekannt. Ein 100-prozentiger Schutz ist jedoch nie möglich.
- Über 90 Prozent des Aufwands sollten Unternehmen und Behörden als Vorbereitung vor einer möglichen Kompromittierung durch Cybercrime betreiben.
- Cybersicherheit ist Chef- bzw. Chefinnensache und keine ausgelagerte Aufgabe der IT-Abteilung.
- Grundsätzlich sollten Unternehmen und Behörden 15–20 Prozent ihres jährlichen IT-Budgets in Sicherheitsmaßnahmen im Bereich Cybersicherheit investieren. Sie schützen damit ihre Existenz und Reputation.
- Unternehmen und Behörden sollten sowohl private als auch staatliche Akteure vor und nach Cybercrimevorfällen einbeziehen. Dies ermöglicht umfassendere Schutzmaßnahmen, die Einleitung von Ermittlungsverfahren gegen die verschiedensten kriminellen Akteure, mit der Zielrichtung der Zusammenarbeit mit internationalen Partnern zur Verfolgung der kriminellen Strukturen.

ca. 148 Mrd. Euro Schaden

sind durch Cyberangriffe und deren Folgen 2023 auf die deutsche Wirtschaft entstanden.

Mehr als 52 % der Unternehmen sehen sich in ihrer Existenz bedroht.

[1] Wirtschaftsschutz 2023 (bitkom.org)

Inhalt

1 Was können Unternehmen und Behörden im Bereich Awareness tun?

Kleine und mittelständische Unternehmen (KMU) sowie kommunale Behörden stehen vor großen Herausforderungen bei der Vorbereitung von Schutzmaßnahmen im Cybersicherheitsbereich. Kompromittierungen entstehen z. B. durch Schadsoftware, Überlastung des Zielsystems durch eine Distributed Denial-of-Service-Attacke (DDoS), Verschlüsselung der Opfersysteme (Ransomware) sowie maliziöse Inhalte zur Beschaffung von Passwörtern, E-Mail-Adressen oder Bankdaten (durch Spam und Phishing)

- **Risikobewusstsein:** Fast jedes Unternehmen ist von den Folgen von Cybercrime betroffen. Grundsätzlich kann jedes Unternehmen und jede Behörde Opfer eines Cyberangriffs werden. Angriffe müssen nicht zwangsläufig gezielt auf eine Organisation gerichtet sein, sie können auch im Rahmen einer größeren Kampagne erfolgen. Außerdem können Daten kleinerer Akteure wertvoll sein, um an größere Akteure heranzukommen. Jedes Unternehmen und jede Behörde sollten sich daher als Teil eines gesamtgesellschaftlichen Ökosystems betrachten. Die Täterinnen und Täter können sowohl von außen als auch von innen, die Tätigkeiten der Organisation kompromittieren. Es gilt daher, einen „Zero-Trust-Ansatz“ zu etablieren. Dieser Ansatz ist eine Cybersicherheitsstrategie, die jedem Akteur misstraut, der auf IT-Ressourcen zugreifen möchte. Somit sollen Datenlecks verhindert und die Sicherheit des Netzwerks erhöht werden.
- **Finanzielle Mitteln:** Grundsätzlich sollten Organisationen 15–20 Prozent ihres IT-Budgets in den Bereich der Cybersicherheit investieren. Das größte Risiko für ein Unternehmen ist die Insolvenz durch Cybercrime. Behörden könnten durch eine Kompromittierung das Vertrauen der Bürgerinnen und Bürger verlieren.
- **Know-how:** Maßnahmen im Bereich der Cybersicherheit sind komplex, dienen jedoch der Aufrechterhaltung des Organisationsbetriebs. Es gilt Vorsorgemaßnahmen zu treffen, bevor ein Sicherheitsvorfall eintritt. Dies verhindert das Ausmaß von Schäden erheblich. Einen hundertprozentigen Schutz wird es jedoch nie geben. Unternehmen in der Cybersicherheit sowie polizeiliche, behördliche und privat-gesellschaftliche Akteure können Organisationen kompetent unterstützen.

Grundsätzlich kann jedes Unternehmen und jede Behörde Opfer eines Cyberangriffs werden!

Unternehmen sollten sich als Teil eines gesamt-gesellschaftlichen Systems betrachten und Vorsorgemaßnah men ergreifen!

Der Bereich Cybersicherheit umfasst Teilbereiche IT-Sicherheit, Prozesse & Strukturen, Human Factor, physische Sicherheit.

Die Akteure sollten ihren Schutzbedarf feststellen, Bedrohungen (Angriffsvektoren) identifizieren, bzw. kennen und eine Risikoanalyse durchführen können, also Bedrohungen auf die eigene IT und bewerten, um im Ernstfall geeignete Maßnahmen zu ergreifen.

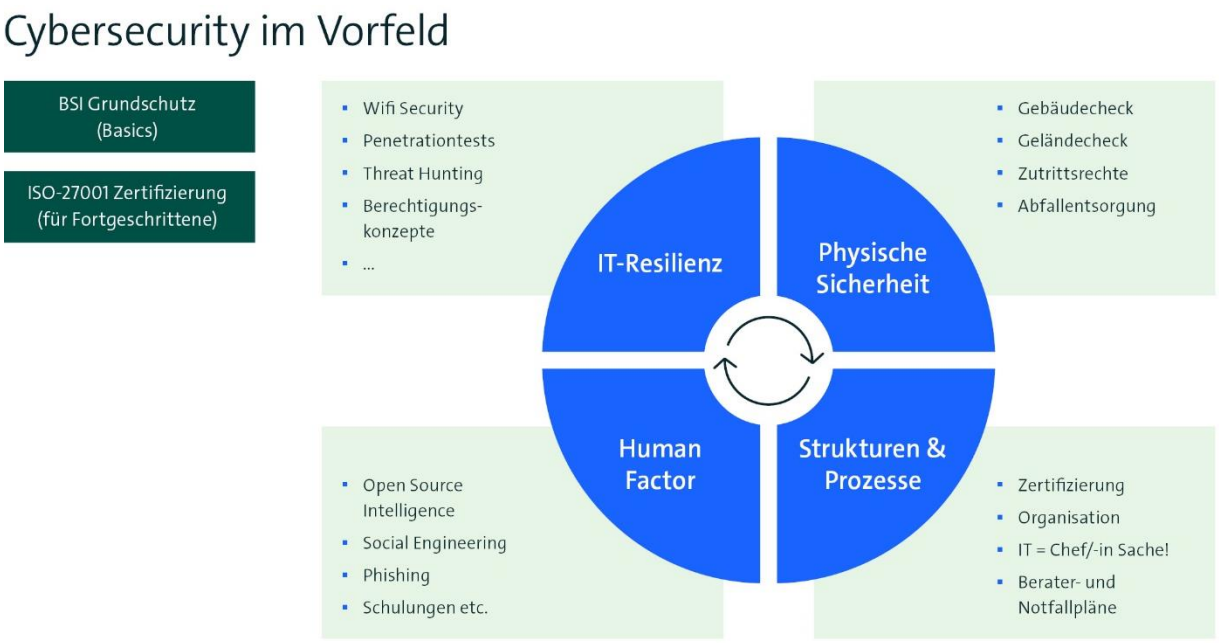


Abbildung 1: Teilbereiche Cybersicherheit im Vorfeld

1.1. Überblick Maßnahmen zur IT-Sicherheit

Im Fokus der IT-Sicherheit von Organisationen steht das Thema Resilienz. Diese reduziert die Komplexität und ermöglicht besser beherrschbare Systeme. Grundvoraussetzung ist ein kompetenter Personalkörper, bzw. der Zugang zu professionellen Partnern.

Maßnahmen:

- **Etablierung des Zero-Trust-Ansatzes**
  - Definition schützenswerter Güter
  - Identifizierung möglicher Angriffsvektoren
  - Endpunktsicherheit (Schutz von Endgeräten wie PCs, Smartphones etc., die auf ein Netzwerk zugreifen können sowie Wifi-Security)
  - Datensicherheit (Schutz von digitalen Datenbanken vor Schäden, Diebstahl usw.)
  - Erstellung eines Zero-Trust-Regelwerkes

  - Berechtigungskonzepte
  - Überwachung und Wartung der Umgebung
- **Backups erstellen**, die Standby- und Hardware-Redundanz, auch am Endpoint, ermöglichen.
- geeignete **präventive Maßnahmen** implementieren und anwenden (Erkennen von Cyberangriffen, Anomalie-Erkennung, Threat Hunting zur Identifikation potenzieller Bedrohungen im Netzwerk, Penetrationstests zur Identifikation von Schwachstellen, Passwort-Guidelines aufstellen, IT-Notfallkarte usw.) und Rechtevergabe der einzelnen Nutzerinnen und Nutzer prüfen (Braucht jede Nutzerin und jeder Nutzer Admin-Rechte?)
- Ernstfälle durch **Szenarien kennen und üben**
  - die Folgen von Situationen auf das Geschäftsmodell antizipieren und in Notfallplänen adaptieren (Notfalldokumentation und Handbücher)
  - geeignete Verträge mit Notfall-Dienstleistern im Vorfeld abschließen und Kontaktwegeüben
  - Definieren einer Notfall-Kommunikation, erprobte Ersatz-Kommunikationswege im Falle einer Kompromittierung eruieren
  - Mitarbeitende im Rollenverständnis, Prioritätensetzung und Richtlinien mit Bezug zur Cybersicherheit schulen
- **Etablierung eines Informationssicherheitsmanagement Systems (ISMS) – am Anhalt der ISO/IEC 27001 bzw. dem IT-Grundschutz des BSI**

  Ebene 1: Strategische Leitlinien (Strategische Bedeutung des ISMS, Beauftragung durch Geschäftsleitung) sowie Definition von Zielen, Grundsätzen und Allgemeinem, Nennung der geltenden Richtlinien
  - Ebene 2: Sicherheitsrichtlinien (Definition und Beschreibung der sicherheitsrelevanten Themenfelder, Nennung zugehöriger Konzepte und geeigneter Nachweise)
  - Ebene 3: Sicherheitskonzepte (Konzepte als Arbeits- und Verfahrensanweisungen mit genaueren Prozessbeschreibungen zur Anwendung und Schulung der Richtlinien)
  - Ebene 4: Nachweise und Aufzeichnungen (Protokolle, Listen und Ergebnisse interner Audits)
- Details und weitere Maßnahmen mit Sicherheitsdienstleistern durchsprechen, einen kostenlosen Erstüberblick kann ggf. auch die Polizei bieten.

Zero-Trust als Grundansatz im Umgang mit Sicherheitsrisiken

1.2 Maßnahmen im Bereich physischer Sicherheit

Cybersicherheit umfasst nicht nur digitale, sondern auch analoge Komponenten für ein Gesamtkonzept. Insbesondere wenn eine Organisation einen gezielten Angriffspunkt darstellt, sei es für andere Unternehmen, ausländische Nachrichtendienste, die organisierte Kriminalität oder weitere Akteure.

Zunächst sollte ein Sicherheitsplanungsprozess durchgeführt werden. Dieser umfasst eine Analyse über mögliche Risiken und Schwachstellen. Auch hier gilt: Organisationen müssen sich ihrer wertvollen Daten und Güter bewusst sein, sodass sich Schutzziele, Sicherheitszonen und einzelne Sicherheitsmaßnahmen ableiten lassen. Allein bei der Auswahl scheinbar banaler Aspekte, z. B. Fensterscheiben (Klassen RC1N – RC6 bzw. einer Zeit zur Überwindung von 1 bis 20 Minuten) oder der Klärung, wer Zugang zum Firmenmüll hat, lassen sich spürbarere Schutzwirkungen erzielen.

Je nach Sicherheitslevel der Organisation sollten auch sämtliche technische Möglichkeiten, z. B. das Abhören mittels Lasertechnologie über Fensterscheiben usw. adaptiert werden, unter Beachtung gesetzlicher Normen und technischer Leitlinien und Standards.

Auch hier gilt die Möglichkeit zur Beratung durch professionelle Dienstleister und die Polizei.

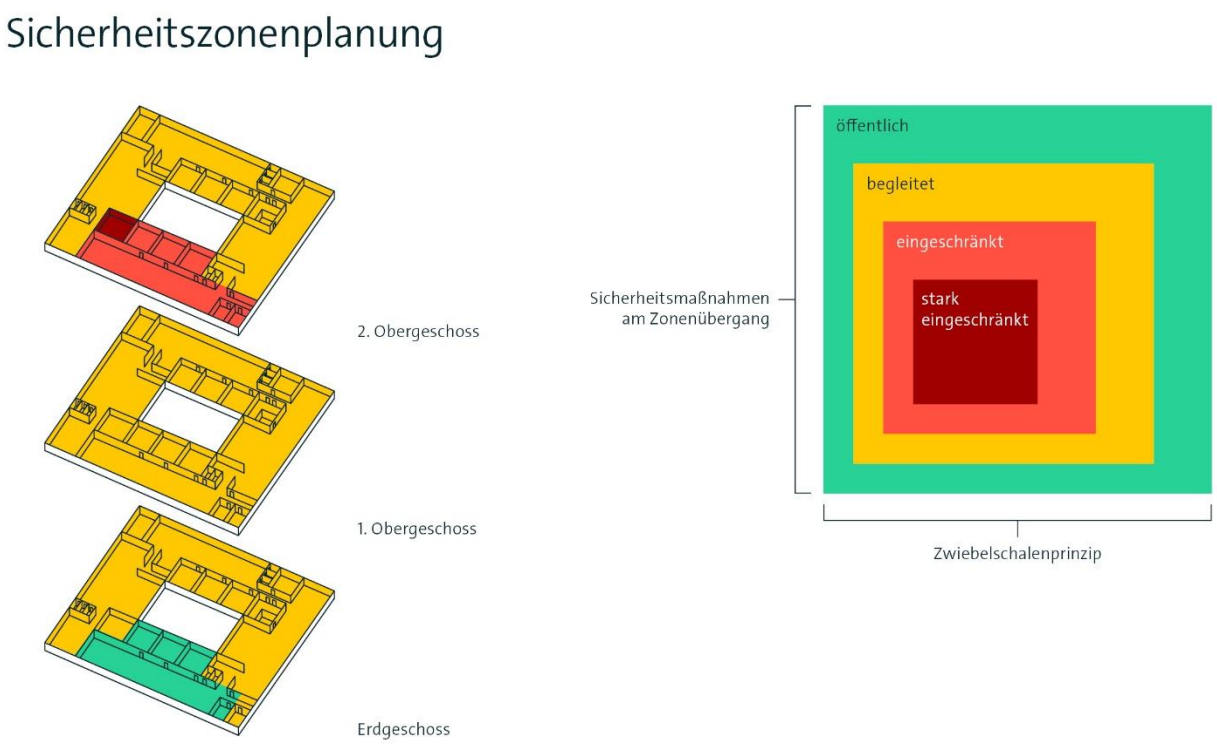


Abbildung 2: Sicherheitszonenplanung

Sicherheitsplanungsprozess

Abbildung 3: Sicherheitsplanungsprozess

Mögliche Sicherheitsmaßnahmen

Abbildung 4: Sicherheitsmaßnahmen

1.3 Maßnahmen im Bereich Human Factor

Zwischenmenschliche Beziehungen sind das Herzstück des gesellschaftlichen und organisatorischen Gefüges. **Der Human Factor ist daher das zentrale Einfallstor zur Kompromittierung der Organisationssicherheit**. Als Basis dient das grundsätzliche Vertrauen zu anderen Menschen, um kollaborativ zu agieren und das natürliche Bedürfnis zur sozialen Interaktion. Cybercrime setzt an dieser Stelle gezielt an.

Grundsätzlich sind soziale Beziehungen von Mitarbeitenden nicht zu kontrollieren. Die gezielte Anbahnung von Kontakten, um an Informationen oder Zugänge zu gelangen, sollte daher stets mitgedacht werden.

Weiterhin folgt das menschliche Handeln Gewohnheiten, Routinen und dem Ansatz, Aufgaben mit geringstmöglichem Aufwand zu erledigen, um Energie einzusparen. Dies kann zu Unachtsamkeiten oder der (un)wissentlichen Umgehung von Prozessen oder Schutzmaßnahmen führen. Awareness kann nicht durch allgemeine Hinweise erreicht werden. Es gilt persönliche Betroffenheit zu erzeugen, um die kognitiven Prozesse, hin zu einer bewussten Verarbeitung von Informationen, dauerhaft zu aktivieren. Dazu eignen sich interaktive Formate, u. a. realistische Plan- und Rollenspiele sowie Übungen.

> Der Human Factor ist das zentrale Einfallstor für Sicherheitsrisiken – Jede Organisation sollte ihr Personal schulen!

Organisationen sollten daher ihr Personal zu diversen Themen mit professionellen Formaten aktiv schulen, um Awareness zu schaffen und Einfallstore zu verringern:

- Social Engineering (z. B. Business E-Mail Compromise)
- Open Source Intelligence und daraus gewonnene Strategien
- Phishing in allen Variationen
- weitere Schulungen zu technischen Themen, Vorgehensweisen von Antagonisten usw.

1.4. Maßnahmen im Bereich Prozesse & Strukturen

Zu geringe Awareness in Organisationen und die daraus resultierende Unterschätzung der individuellen Angriffsgefahr bzw. Angriffswahrscheinlichkeit (schwächstes Glied einer Kette) führen zu nicht geeigneten oder gar nicht vorhandenen Schutzmaßnahmen.

Auch wird das Thema Cybersicherheit oft als alleinige Aufgabe der IT-Abteilung, u. a. der Informationssicherheitsbeauftragten, gesehen, welche ggf. selbst diese Aufgabe aufgrund fehlender Separation von Verantwortlichkeiten nur als Nebentätigkeit vollziehen. Verantwortung innerhalb der Strukturen ist klar zu definieren, und deren Ausübung zu kontrollieren, um geeignete Maßnahmen abzuleiten.

- Es gilt: **Cybersicherheit ist Chef- bzw. Chefinnensache Sache und daher nicht delegierbar. Das Vorbild der Chefin bzw. des Chefs trägt maßgeblich zur Akzeptanz von IT-Sicherheit innerhalb der Belegschaft bei. Die Integrität des gesamten Geschäftsmodells hängt von der Cybersicherheit ab.**

- **Im Sektor der Kritischen Infrastrukturen (KRITIS-Sektor) gibt es gesetzliche Vorgaben und Richtlinien für Sicherheitsvorgaben, welche auch für Behörden gelten sollten**, da diese ein Teil der KRITIS sind.
- Organisationen können weiterhin prüfen, ob gewisse Zertifizierungen wie die ISO 27001 für sie sinnvoll sind, welche u. a. Grundvoraussetzung für fast alle Cyberversicherungen ist, bzw. schaffen diese Zertifizierungen oft Grundvoraussetzungen für die Interaktion mit staatlichen Stellen als Auftraggeber. **Die Standards des BSI-Grundschutzes umzusetzen, sollten selbstverständlich sein.**
- **Organisationen sollten professionelle Beratungen, sei es durch private oder staatliche Akteure, einbeziehen** und auch im Vorfeld deren Erreichbarkeiten im Notfall absprechen.
- **Schließlich gilt es auf die Organisation zugeschnittene Notfallpläne zu erstellen und diese zu üben.** Daraus lassen sich Einzelmaßnahmen, z. B. Klassifizierung von Notfällen und daraus abgeleitete Alarmketten, die Zusammensetzung eines Krisenstabes, Erstmaßnahmen im Krisenfall, Umgang mit Lösegeldzahlungen, versicherungstechnische Angelegenheiten etc. ableiten.

Cybersicherheit ist Chef- bzw. Chefinnensache und nicht die der IT-Abteilung!

1.4.1. Der Notfallplan

Organisationen haben grundsätzlich die Möglichkeit, kostenlose Einblicke in die Gestaltung von Notfallplänen zu erhalten. Als Anhalt dienen u. a. Vorlagen des BSI, der Allianz für Cybersicherheit oder das Muster anbei.

Notfallpläne

1. Vorbereitung

- Wer ist zuständig IT-Sicherheit | Notfallmanagement?
- Welche Erstmaßnahmen treffen Sie? (Alarmierung | Meldewesen | Notfallkontakte und Rollen)
- Vorbereitung externer Meldepflichten (Datenschutz | KRITIS)
- Risiko & Businessrisiken betrachten (was soll geschützt werden & was passiert wenn x nicht mehr funktioniert | Disaster Recovery-Plan (DR) - Backup-Strategie (Strom, Datencenter etc.)
- Was deckt Ihr IT-Dienstleister ab?
- Liste Ansprechpartner*innen zzgl. Erreichbarkeit anfertigen
- Regeln der Kommunikation nach Innen und Außen festlegen
- Überwachungsmaßnahmen IT-Landschaft prüfen
- Üben Sie Notfallszenarien
- Prüfung der Infrastruktur auf Angreifbarkeit | Schulungskonzepte der Mitarbeitenden | Sicherheitsupdates aktuell? etc.
- Inventar IT-Infrastruktur (Netzplan)
- Wer hat Benutzungsrechte und wie sind interne Netze vernetzt?

2. Bereitschaft

- regelmäßige Überprüfung des Sicherheitsstatus ihrer Systeme
- Sicherstellung der Bekanntheit und Erreichbarkeit von Ansprechpartnern bei IT-Notfällen (↗ BSI - IT-Notfallkarte (bund.de))
- Prüfen Sie Pläne auf Resilienz des Personals (Die Aufarbeitung nach einem Angriff kann Monate dauern nicht Tage!)

3. Bewältigung

- Kontaktierung festgelegter Ansprechpartner*innen die zur Bewältigung nötig sind
- Einbeziehung Betroffener (Beobachtungen | Aktivitäten)
- Kommunikation nach Innen & Außen
- Nehmen Sie Mitarbeitende aktiv mit!
- Verbindungsaufnahme IT-Dienstleister
- Sammeln und sichern Sie Systemprotokolle, Logdateien, etc.
- Dokumentation Sachverhalte, die mit dem Notfall in Zusammenhang stehen könnten
- Verbindungsaufnahme mit den ZACs der Polizeien, sowie freiwillige Meldungen an die ACS | bei vermuteter Spionage Verfassungsschutz alarmieren
- Beachten Sie Meldepflichten

4. Nachbestellung

- Schließen Sie aufgedeckte Schwachstellen und Sicherheitslücken
- Überwachen und monitoren Ihrer Netzwerke und IT-Systeme
- Nach der Krise ist vor der Krise – Lessons Learned aufbereiten (Regelungen, Prozesse, Maßnahmen prüfen)
- Dokumentationen zum Notfallmanagement
- Stärkung der IT-Sicherheitsarchitektur
- Kommunikation nach Innen & Außen
- Nehmen Sie Mitarbeitende aktiv mit!

Abbildung 5: Notfallplanübersicht

Einzelheiten sind mit einem Unternehmen der Cybersicherheit im Detail zu klären. Erste Beratungen können ggf. auch die Zentralen Ansprechstellen Cybercrime (ZAC) in den Landeskriminalämtern der Länder oder für den KRITIS-Sektor sowie das Bundeskriminalamt durchführen.

Dabei gilt:

- **Es gibt keine Blaupause für einen Notfallplan**. Nach Feststellung der schützenswerten Daten und Güter gilt es, den Plan auf die Bedürfnisse der Organisation abzustimmen.
- **Der Notfallplan sollte kurz und präzise sein**. Er muss in regelmäßigen Abständen überprüft, angepasst und aktuell gehalten werden und auch als analoge Rückfallebene vorliegen. Für den Notfall, der meist dynamisch ist, lassen sich im Vorfeld stets nur erste Maßnahmen adaptieren.
- **Der Notfallplan ist zu üben, damit im Ernstfall alle Akteure Abläufe und Rollen kennen.**
- **Der Notfallplan sollte alle nötigen Stakeholder erfassen und vor allem Meldepflichten, z. B. bei Verstößen zum Datenschutz, vorbereiten.**

Halten Sie Notfallpläne übersichtlich und üben Sie diese!

1.4.2. Der Krisenstab

Auch der Krisenstab ist an die jeweilige Organisation zu adaptieren. Ein Beispiel zeigt die folgende Grafik.

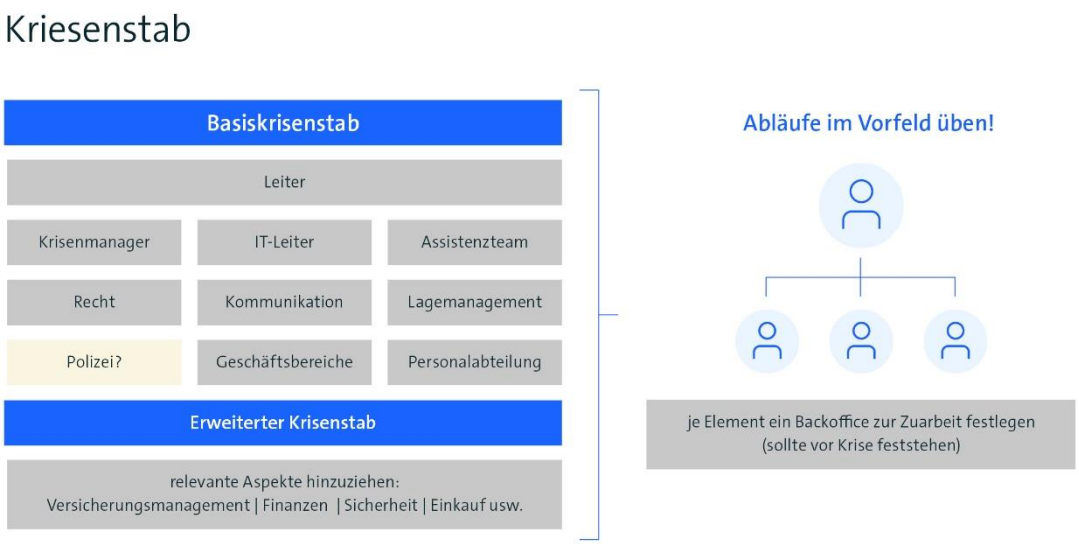


Abbildung 6: Beispiel eines Krisenstabs

Der Krisenstab kann aufgeteilt werden. Ein Basiskrisenstab wird z. B. bei allen ernsten Vorfällen aktiviert und sollte über vorher zugewiesenes und eingewiesenes Personal verfügen. Anhalt dazu gibt das BSI: Der Leitungsstab sollte durch Kernteams thematisch beraten werden. Empfehlenswert sind u. a. ein IT-, Notfall- und Krisenkommunikationsteam sowie ein Team zum Thema Personal. Die Ausrichtung der

Teams obliegt den Möglichkeiten der Organisation.[2] Diese soll die vordergründigen Akteure unterstützen. Zu diesen Akteuren könnten u. a. zählen: IT bzw. IT-Sicherheitsbeauftragte, Datenschutzbeauftragte, Geschäftsleitung und weitere Personen (z. B. Unternehmenskommunikation oder PR). Ein erweiterter Krisenstab kann ereignisabhängig einberufen werden.

Es ist zu beachten:

- **Cybervorfälle können eine Organisation über Monate binden. Der Krisenstab sollte daher resilient geplant werden.** So sollten einzelne Stabselemente auch über Arbeitsgruppen oder Back-Office-Teams verfügen, welche zuarbeiten und Arbeitsaufträge ausführen.
- **In der Krise ist Kommunikation entscheidend**[3] (mangelnde Kommunikation führt z. B. zu Gerüchten, Stresssituationen für Mitarbeitende, unkontrollierte Information von Stakeholdern usw.)
- **Der Erfolg des Krisenstabes, mit einer Krise umzugehen, liegt in der Vorbereitung** (Meldepflichten, Kommunikationswege, Stakeholder-Identifikation, Erstmaßnahmen usw.) In der Krise ist die Dynamik sehr hoch, was zu kostspieligen Fehlentscheidungen bei spontanen Bewertungen führen kann.

1.4.3. Erstmaßnahmen im Krisenfall

Kein Cybervorfall gleicht dem anderen. Dennoch ist es sinnvoll, sich im Vorfeld mittels von Szenarien etc. auf Angriffsvektoren vorzubereiten.

Organisatorische Maßnahmen:

- Ruhe bewahren – keine falsche Angst (Vorfall über vorgesehene interne Meldewege z. B. an die IT oder Informationssicherheitsbeauftragte melden)
- Auswirkungen feststellen
  - Kerndienstleistung betroffen? (Risikoklassifizierung nach ISMS oder Notfallplan)
  - Strafrechtlich relevant?
  - Kundschaft oder Partner betroffen?
  - Handlungsbedarf?
  - Klassifizierung der Bedrohung, um weitere Maßnahmen einzuschätzen
- Sicherheitsbeauftragte, Krisenstab oder Task Force einberufen und Aufgaben festlegen

Beachten sie im Krisenfall Melde-pflichten, ihr Personal und ihren Notfallplan.

Der Erfolg hängt von der Vorbereitung ab!

[2] BSI-Standard 200-4
[3] BMI - Publikationen - Leitfaden Krisenkommunikation (bund.de)

- Termine und Fristen überwachen
  - z. B. Meldepflichten zu Datenschutz bzw. DSGVO?
  - BSI/KRITIS?
  - freiwillige Meldung, z. B., um weitere potenziell gefährdete Organisationen warnen zu können?
  - Vertragliche Informationspflichten?
  - Meldung an Versicherungen?
  - an Kundschaft, Auftraggeber oder Partner?
  - Beachtung sonstiger Compliance-Regeln?
- Weitere Informationen sammeln
  - Was ist passiert?
  - Wie und wo ist es aufgefallen?
  - Wurde der Vorfall intern oder extern gemeldet?
  - Kontakt halten zu meldenden Personen (Dabei ist es wichtig, diese sind nicht als Täterinnen oder Täter zu betrachten, z. B. bei einem unbeabsichtigten Klick auf einen Link einer Phishingmail)
- Interne Informationsketten gemäß Notfallplan zu Mitarbeitenden (Sprachregelung intern vs. extern – aktiv vs. reaktiv)
- Externe Kommunikationsstrategien bereits im Voraus planen – Informationen gelangen fast immer nach Außen
- Polizei oder Landeskriminalamt (LKA) – Stellen einer Strafanzeige? Im Zweifelsfall Kontaktaufnahme mit der Zentralen Ansprechstelle Cybercrime (ZAC) beim jeweiligen LKA
- Externe Unterstützung benötigt (Incident Responce Team oder Dienstleister)? Diese Unterstützung sollte bereits vor dem Vorfall geklärt sein. Dienstleister und Fachpersonal sind rar und stark eingebunden. Lernen diese die Organisation erst im Notfall kennen, kostet es vor allem wertvolle Zeit. Es gilt, schnell zu handeln.
- Forensische Sicherung für IT-Dienstleister und Polizei und zur Nachbereitung bzw. Aufarbeitung, um künftig vergleichbare Vorfälle zu vermeiden
  - Log-Dateien, Screenshots, Fotos, Videos, Speicherabbildungen und Notizen zum Vorfall

Technische Maßnahmen

- Betroffene Systeme vom Netzwerk und vom Internet trennen? (Achtung diese Entscheidung ist Chefinnen- bzw. Chefsache, da die Gefahr besteht, bei Ransomware den Verschlüsselungsprozess zu unterbinden und somit die Daten unwiderruflich unbrauchbar zu machen)
- Geräte nicht herunterfahren
- Keine Anmeldung mit privilegierten Rechten. Existieren Benutzerkonten mit privilegierten Rechten? Gibt es Hinweise, dass privilegierte Rechte unbefugt eingerichtet und genutzt wurden?
- Betroffene Systeme identifizieren und Ausmaß feststellen (Existieren Außenstellen, die kompromittiert sein könnten? Sind Mitarbeitende im Urlaub, die es zu informieren gilt?
- Infizierte Systeme als vollständig kompromittiert betrachten, d. h. komplette Neuinstallation durchführen
- Alle auf betroffenen Systemen gespeicherten Zugangsdaten als kompromittiert betrachten
- bei kompromittiertem Active Directory (AD) ganzes Netzwerk als kompromittiert betrachten, somit vollständig neu aufsetzen
- Notbetrieb, Neuinstallation, Wiederanlauf
- Backups zunächst unterbinden, da Schadsoftware mit gesichert werden könnte, was das Backup kompromittiert, vorhandene Backups unbedingt vorher checken, ob diese nicht kompromittiert sind.

1.4.4 Umgang mit möglichen Lösegeldforderungen

Grundsätzlich sollten Organisationen keine Lösegeldzahlungen leisten. Die Praxis ist jedoch eine Grauzone, gerade, wenn die wirtschaftliche Existenz bedroht ist. Im Fokus steht oft der Mittelstand. Die Entscheidung zur Zahlung kann den Verantwortlichen nicht abgenommen werden. Das Für und Wider gilt es abzuwägen.

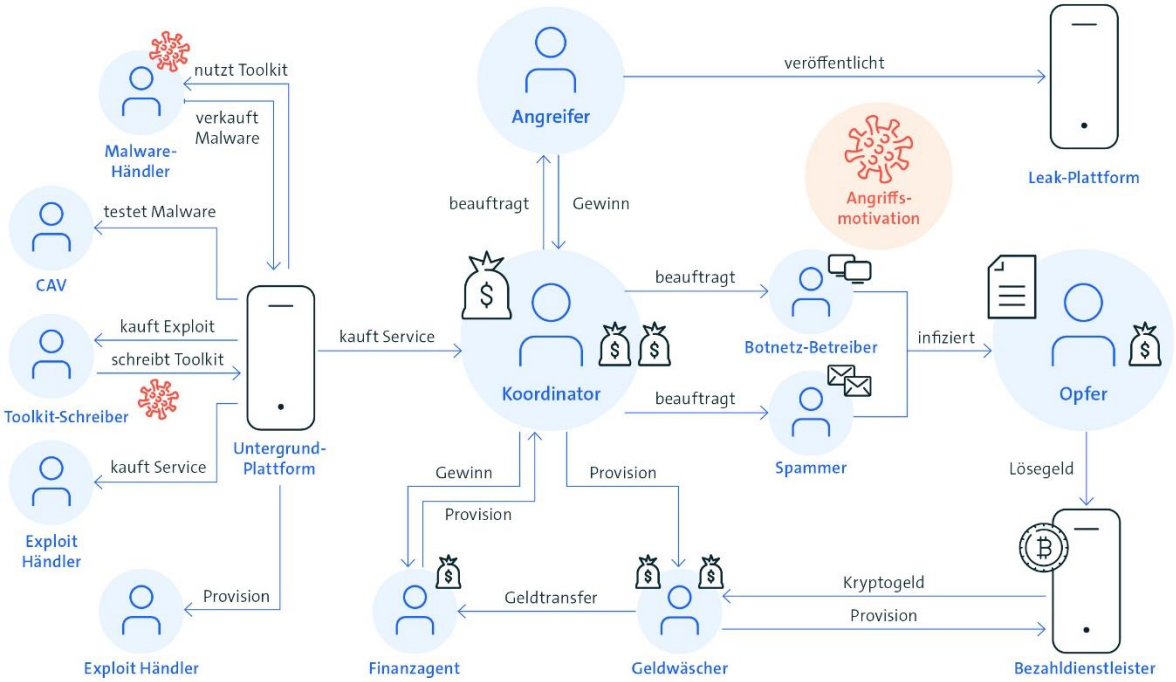
Abbildung 7: Lösegelder

Organisationen sollten sich im Vorfeld über den Umgang mit der Thematik Gedanken machen, u. a. auch welche Folgen eine Nichtzahlung hätte oder wie im Ernstfall nötige Kryptowährungen beschafft werden. Dabei gilt Bitcoin bislang als meist genutzter Standard. Organisationen können dies auch in hypothetischen Szenarien mit den Polizeibehörden, wie dem Bundeskriminalamt, erörtern, dabei ist jedoch das Legalitätsprinzip der Polizei zu beachten (Ermittlungen sind einzuleiten, sobald eine Straftat bekannt wird).

Bei Angriffen mit Ransomware verschlüsseln Cyberkriminelle Daten, um sie gegen die Zahlung eines Lösegelds wieder zu entsperren. Die Höhe von Lösegeldforderungen variiert und kann in die Millionen gehen. Kriminelle Strukturen agieren dabei im höchsten Maße professionell und nach wirtschaftlichen Grundsätzen. Es gilt, entstandene Kosten für Angriffe zu decken und Profite zu maximieren. Einen Überblick der Strukturen von Cybercrime-as-a-Service bietet die Grafik des Landeskriminalamtes Sachsen.

Unternehmen sollten keine Lösegelder zahlen, sie könnten sich strafbar machen. Die Realität ist jedoch eine Grauzone.

Cybercrime as a Service ein grober Einblick



Quelle: basierend auf Angaben des Landeskriminalamtes Sachsen

Abbildung 8: Cybercrime-as-a-Service ein grober Überblick

Erhebungen zu Lösegeldzahlen, durch einzelne Cybersicherheitsunternehmen, können als unverbindlicher Anhalt zur Veranschaulichung dienen. Die durchschnittliche Lösegeldsumme beträgt nach einzelnen Erhebungen weltweit ca. 404.000 US-Dollar, mit steigender Tendenz. Da immer weniger Organisationen zahlen, treibt dies die Kosten für die Cybercrime-Strukturen. Weltweit zahlen laut dieser Erhebungen ca. 41 Prozent der Firmen Lösegelder, wobei Europa mit elf Prozent die geringste Zahlungsbereitschaft aufweist.[4]

Ransomware-Gruppierungen sind im Grunde bekannte Akteure, jedoch ohne feste Organisationsstrukturen und oft aus dem Ausland agierend, was deren Verfolgung erschwert. Die Masse aller Angriffe lässt sich auf wenige Kollektive zurückführen. Auch agieren Netzwerke mal als wirtschaftliche Akteure und mal als politische Akteure, u. a. im Auftrag Russlands, um Strukturen und Prozesse zu stören. Insbesondere chinesische Gruppen, agieren meist im staatlichen Auftrag, um Know-how abzuschöpfen, weniger im Bereich von Ransomware.

Das Vorgehen der Erpresser hat sich weiterentwickelt. Datenverlust war meist das einzige Druckmittel gegenüber Organisationen. Heute drohen die Kriminellen auch mit der Veröffentlichung der Daten oder drohen mit Erpressungen von Geschäftspartnern und Kundschaft der Organisationen (sog. Double- bzw. Triple-Extortion**). Betroffenen muss jedoch klar sein, unabhängig davon, ob eine Lösegeldzahlung eine**

[4] Aufgrund der Gleichbehandlung von Mitgliedsunternehmen im Bitkom werden einzelne Firmen, von denen die Zahlen stammen, nicht genannt.

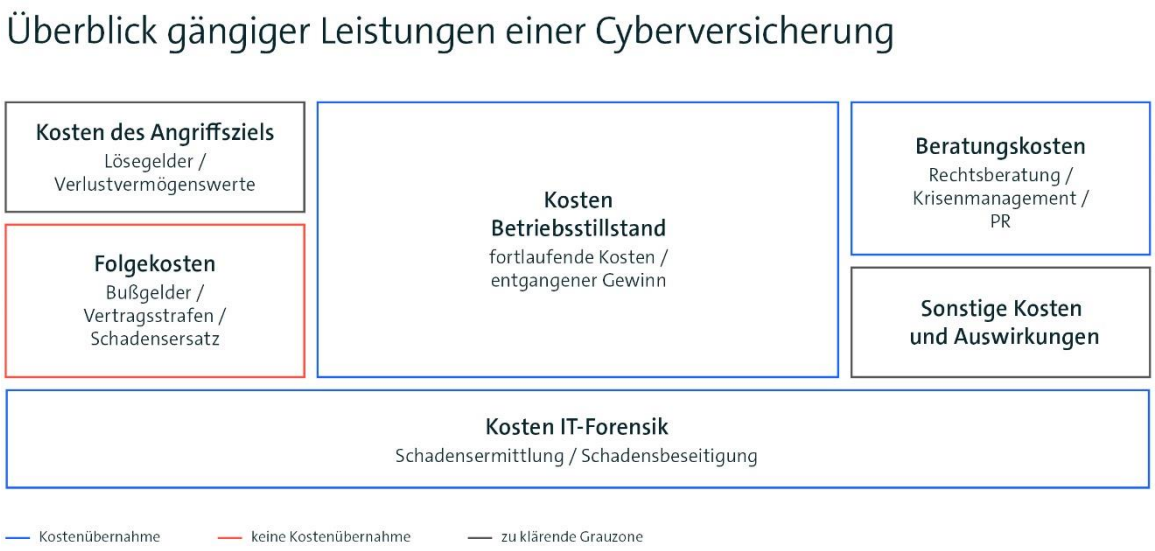
Veröffentlichung im Netz verhindert, sind die Daten bereits kompromittiert. Sie sind durch den Abfluss aus der Organisation in den Weiten des Netzes und daher nicht als Paket zu betrachten, welches nach Zahlung ohne Folgen einfach wieder zurückkehrt. Die Einbeziehung der Polizei sollte geprüft werden, denn diese kann veröffentlichte Unternehmensdaten ggf. Foren oder Gruppierungen zuordnen und neben den IT-Experten weitere Hinweise zum Umgang mit der Situation bieten.

1.4.5. Die Cyberversicherung

Die Sicherheitskooperation Cybercrime führt keine Beratung über Cyberversicherungen durch. Organisationen müssen dies stets mit qualifizierten Beratenden der Versicherungsbranche erörtern.

Grundsätzlich gilt: Unternehmen können sich gegen Cyberkriminalität entweder durch die Ergänzung von Cyber-Komponenten in der betrieblichen Haftpflichtversicherung oder den Abschluss einer vollständigen Cyber-Police schützen. Das Leistungsspektrum einer Cyberversicherung erstreckt sich dabei über die Deckung von Eigenschäden, Drittschäden und zusätzliche Service- Leistungen.

Abbildung 9: Überblick Zahlungsinhalte



Zu Eigenschäden zählen z. B. die Kosten für die Reparatur von IT-Systemen, die Neubeschaffung von Hardware oder die Gehälter von Beschäftigten in Folge einer Betriebsunterbrechung. Eine Cyberversicherung übernimmt auch die Kosten für Sachverständige, die versuchen, die Daten wiederherzustellen.

Versicherungsunternehmen bieten zusätzlich zur Zahlung von Eigen- und Drittschäden auch Service-Leistungen an, die einem Unternehmen nach einem Hackerangriff beim Krisenmanagement helfen. Dazu zählen neben der Beweissicherung durch IT-Spezialisten auch die Begrenzung von Folgeschäden durch gerichtliche Auseinandersetzungen oder Imageschäden.

Der Weg zur Cyberversicherung ist nicht mit dem Abschluss einer normalen Versicherung zu vergleichen. Organisationen müssen eher nachweisen, dass sie versicherungsfähig sind. Viele Versicherer verlangen daher die vorherige Umsetzung von Grundstandards, min. des BSI-Grundschutzes. Oft bedarf es einer Zertifizierung nach ISO 27001. Mittels eines komplexen Fragebogens gilt es den Nachweis zu erbringen, wobei dieser Fragebogen mit professionellen Sicherheitsdienstleistenden gemeinsam beantwortet werden sollte. Werden Antworten nicht wahrheitsgemäß bearbeitet, sei es bewusst oder unbewusst durch technische Unkenntnis, kann dies zum späteren Ausschluss der Zahlung führen (Angaben fallen unter die vorvertragliche Anzeigepflicht gemäß §19 VVG.). Jeder Versicherer kann dabei einen eigenen Fragebogen, mit unterschiedlichen Themenkomplexen, haben. Den Versicherern sind oft vorhandene Notfallpläne, Offline-Backups, Restore-Tests und weitere aufgezeigte Aspekte der Awareness wichtig.

Organisationen sollten daher ein Cybersicherheit-Assessment durchführen. Dieses umfasst die Sichtung der Unterlagen und Aufbereitung der Fragen, Gespräche mit Expertinnen und Experten sowie die Anforderung von Nachweisen, zur Erstellung einer finalen Angebotsanfrage.

Ab wann eine Cyberversicherung sinnvoll ist, müssen Unternehmen individuell bei Vorlage eines Angebots abwägen. Eine gesetzliche Pflicht zur Cyberversicherung besteht aktuell nicht.

- Sieht eine Versicherung eine Eigenbeteiligung vor?
- Wie hoch ist die Prämie? Aufgrund stets steigender Schadsummen, steigen auch ggf. jährlich die Prämien. Für gewöhnlich orientiert sich diese an der Branche, am Umsatz, Schadenserfahrungen, der Versicherungssumme, dem Risiko für den Versicherer usw.
- Welchen Service bieten Versicherer an? (24/7-Hotline, Rechts- und PR-Beratung, Forensik, technische Schadenermittlung usw.)
- Achtung: Viele Versicherer haben auch eine sogenannte Kriegsklausel. Sie schließen so staatlich gelenkte Cyberangriffe aus der Deckung aus. Dies wurde bereits vor dem Ukraine-Konflikt beschlossen. Solche Versicherungsgesellschaften argumentieren, dass sie z. B. Zahlungen bei Cyberangriffen von russischen oder ukrainischen Hackern verweigern, weil das Kriegshandlungen seien. Das stößt auf Unverständnis in der Wirtschaft. Die Handlungen der Hacker lassen sich zwar grob lokal verorten, aber oft nur schwer mit staatlichen Stellen in Verbindung bringen. Auch kann der genaue Ursprung des Angriffs verschleiert worden sein. Der Versicherer ist hier in der Beweispflicht, was sich schwierig gestalten und Streitpunkte bieten kann.
- Ein Cyberangriff ist leider nicht vorhersehbar, daher müssen im Vorhinein klare Absprachen zwischen einer Organisation und Versicherungsanbieters getroffen werden. Nach einem Angriff muss es schnell gehen und das Notfallmanagement reibungslos funktionieren. Die Erfahrungswerte und die Routine einer Cyberversicherung sind in der Praxis ein nicht zu unterschätzender Mehrwert für betroffene Organisationen.
- Bei Großunternehmen ist zu klären, inwiefern ein Versicherungsanbieter den Schaden überhaupt tragen kann.

Seminare zum Thema lassen sich u. a. bei der Bitkom-Akademie unter http://www.bitkom-akademie.de/ finden, bzw. individuell für die Organisation vereinbaren: mailto:info@bitkom-akademie.de

2 Was kann die Polizei für Organisationen tun?

Insbesondere wirtschaftliche Organisationen stehen der Kontaktierung der Polizei bei Cybersicherheitsvorfällen oft skeptisch gegenüber. **Oft ist unklar, was die Einbeziehung der Polizei im Vorfeld oder eine Strafanzeige bei einem Vorfall bezwecken kann.**

Grundsätzlich verfügen Unternehmen im gewerblichen Cybersicherheitsbereich über:

- Erstzugriff auf Datenspuren
- Kenntnis der Opfersysteme
- Nähe oder Vertrauen zu Geschädigten

Fähigkeiten Polizei mit der Justiz

- International ermitteln
- Datenerhebung von Internet Service Providern
- Deanonymisieren des Täters
- Zerschlagung der Infrastruktur

Polizei und Cyber-sicherheitsanbieter ergänzen sich und stehen nicht in der Konkurrenz.

Auszug der Möglichkeiten der Polizei im Bereich Cybercrime

IT-Ermittlungen

- herausragende komplexe Ermittlungsverfahren der »qualifizierten Cybercrime« (Cybercrime im engeren Sinn)
- Eigene Ermittlungszuständigkeit (Land) Ransomwareangriffe auf Wirtschaft und Behörden, etc. (nicht Privatpersonen)
- Entgegennahme von Sicherheitsvorfällen mit Bezug zu Cybercrime (telefonisch oder per Mail) und Einleitung von Sofortmaßnahmen-ZAC »operativ«

IT-Auswerteunterstützung

- Aufbereitung von Verkehrsdaten der Telekommunikation – insbesondere von Funkzellendaten zur weiteren Analyse, z. B. zur Erstellung von Bewegungsprofilen und zur gerichtsverwertbaren Visualisierung
- Unterstützung der Vorgangssachbearbeiter bei der Auswertung von Daten durch:
  - gezielte Aufbereitung und Analyse von Daten
  - Beratung und methodische Unterstützung
  - Bereitstellung und Integration unterschiedlicher interner und externer Datenquellen

Telekommunikationsüberwachung

- TKÜ-Maßnahmen und Verkehrsdatenerhebungen
- Erhebung von Bestandsdaten
- Identifizierung unbekannter Mobilfunkanschlüsse
- Lokalisierung von bekannten Mobiltelefonanschlüssen / -geräten
- Funkzellenerhebung Funkzellenanalyse
- Analyse von WLAN-Netzwerken

IT-Forensik

- Computerforensik, z.B.
  - forensische Sicherung PC
  - Entschlüsselung
  - Analyse von Malware
- Mobilfunkforensik, z. B.
  - forensische Sicherung mobiler Endgeräte
  - Umgehen von Passwortsperren bei Smartphones
  - Chip-Off-Forensik
- Internet-und Netzwerkforensik, z. B.
  - Forensische Sicherung aus dem Netz
  - Kryptowährungen
  - Quellcodeanalyse

Abbildung 10: Fähigkeiten der Polizei

Zum anderen gibt es noch immer diverse Vorbehalte zur Tätigkeit der Polizei:

- Mitnahme von Hardware bzw. Störung der Organisationsabläufe
- Erscheinen der Polizei vor Ort mit großer Öffentlichkeitswirksamkeit
- Zufallsfunde führen zu Ermittlungen und Strafbarkeit
- Die Polizei anzurufen, bringt nichts
- Verlust der Presse-Souveränität
- Verlust der Handlungsfreiheit

Unternehmen sollten die Polizei vor, während und nach einem Vorfall einbeziehen.

Hier ist klar zu sagen: Dies sind Mythen. Organisationen sollten die Zentralen Ansprechstellen Cybercrime (ZAC) der Polizei stets einbeziehen.

Die Polizei hat den Fokus auf die Strafverfolgung der Täter und nicht auf die Einhaltung von bspw. IT-Sicherheitsrichtlinien der geschädigten Institution. Im Vorfeld kann die Polizei einen ersten Überblick zu Awareness-Maßnahmen schaffen. Dies schafft Organisationen Sicherheit, bevor sie sich professionellen Dienstleistern zuwenden, um mit denen auf Augenhöhe zu sprechen. Im Ernstfall kann die Polizei zusammen mit Dienstleistern Maßnahmen ergreifen, wird jedoch keine IT-Systeme wieder herstellen. Diese stehen in keiner Konkurrenz, sondern ergänzen sich. Auch eine Nachbereitung ist mit der Polizei gestaltbar: Was lief gut, was kann verbessert werden?

Was braucht die Polizei von Organisationen nach einem Cybervorfall?

Personendaten des Mitteilers und weiteren essenziellen Zeugen

- vollständiger Vor- und Nachname
- Geburtsdatum und Geburtsort
- ladungsfähige Anschrift
- telefonische Erreichbarkeit
- Beschreibung der Funktion innerhalb der geschädigten Firma (z. B. Geschäftsführerin bzw. Geschäftsführer oder Buchhalterin bzw. Buchhalter etc.)

Ansprechpartnerinnen- und Partner und deren Erreichbarkeiten

- Interne oder externe IT-Verantwortliche der geschädigten Institution, Vertreterinnen und Vertreter des Unternehmens, justizielle Ansprechpartnerinnen- und Partner, weitere relevante Personen

Sachverhalt

- Detaillierte Beschreibung des Vorfalls inklusive aller getätigten Maßnahmen und einer Zeitleiste (insbesondere Zeitpunkte von: Letzte Systemverfügbarkeit, Ereigniszeitpunkt, Feststellungszeitpunkt), dazu ggf. Schadensaufstellung oder Abschätzung dazu, Informationen zu und von Täterinnen und Tätern, über betroffene Systeme, außerdem Informationen zu Niederlassungen, Abteilungen und möglichen Folgen (weitere Systemausfälle, mittelbar betroffene Systeme, Kundinnen und Kunden, etc.)

Maßnahmen

- Vermeiden des Verlustes von Protokolldateien (sichern), Ereignisprotokoll (z. B. Änderungen an Systemen)

Ermittlungen vor Ort

Abschließbarer Raum für polizeiliche IT-Forensik, Internet, Parkplatz

Schließlich ist auch hier wieder aufzuführen, dass jede Organisation Teil eines gesamtstaatlichen, resilienten Ökosystems ist. **Strafanzeigen dienen in erster Linie der Sicherstellung eines Strafverfahrens im Hinblick auf die Ermittlung der Täterin bzw. Des Täters und z. B. der Zerschlagung krimineller Organisationsstrukturen. Weiterhin helfen sie bei der Erstellung eines bundesdeutschen Cyberlagebildes, welches sowohl länderübergreifend (zwischen Landeskriminalämtern), als auch zwischen der Bund-Länderebene (Bundeskriminalamt-Landeskriminalämter), thematisiert wird.** Dies dient auch einer internationalen Abstimmung, z. B. mit dem Federal Bureau of Investigation (FBI), und führt zu Ermittlungserfolgen.

Gestellte Anzeigen führen zur Erhellung des Dunkelfeldes, wobei schätzungsweise mehr als 90 Prozent aller Straftaten im Cyberraum nicht bekannt sind. Dies führt auch zur Stärkung der personellen Ressourcen der Polizei, die sich oft aus der Polizeistatistik ableiten. Schlagfertige Sicherheitsbehörden liegen im gesamtgesellschaftlichen Interesse. Deren Befähigung lässt sich jedoch auch durch eine noch stärkere

Kooperation und Vernetzung eines gemeinsamen Ökosystems aus Staat-Wirtschaft-Wissenschaft intensivieren.

3 Was ist im Umgang mit Sicherheitsunternehmen zu beachten?

Viele Organisationen scheuen sich, professionelle Dienstleister im Bereich der Cybersicherheit einzubeziehen. Hintergrund ist oft die Annahme, Risiken selbst bewältigen zu können, mangelnde Awareness, u. a. auch durch zu wenig Know-how zur Lageeinschätzung, aber auch das Kostenargument.

Wie aufgezeigt, sollten Organisationen antizipieren, was das für sie größte Risiko einer Kompromittierung ist. Für wirtschaftliche Akteure ist dies die Insolvenz. Für andere Akteure der Verlust von Vertrauen und Reputation.

Bei der Auswahl von Dienstleistern sollte berücksichtigt werden:

- Eine Auswahl vor einem Sicherheitsvorfall treffen. Dies fördert neben dem Vertrauen der Partner auch die Kenntnis von Strukturen und Prozessen innerhalb der Organisation und führt zu tiefgreifenderen Sicherheitsmaßnahmen, bzw. zur späteren Minimierung von Schäden.
- Auf die personelle, zeitliche und räumliche Verfügbarkeit von Dienstleistern achten (Wann, kann wer, wo sein?)
- Referenzen von Dienstleistern beachten (u. a. auch Zertifizierungen und geeignetes Personal, oder ob der Dienstleister ggf. bereits Partner der Polizei oder eigener geschäftlicher Kontakte ist, usw.).
- Regelmäßig Verbindung halten, um Neuerungen in der Organisation oder beim Dienstleister zu adaptieren und die Sicherheit zu stärken.
- Anfallende Honorare nicht als Kosten, sondern als Investition in die Funktionsfähigkeit der Organisation betrachten.
- Kriterien zur Auswahl finden sich auch beim BSI[5]

Wo lassen sich Dienstleister finden?

- über das BSI

Organisationen sollten Sicherheits-dienstleister vor dem Schadensfall einbeziehen, um das Ausmaß zu begrenzen.

[5] APT-Response-Dienstleister (bund.de)

- über Handelskammern
- über Wirtschaftsverbände (z. B. Durchsicht der Mitgliedschaft)
- Referenzen von Partnern

4 Anhang: Ansprechstellen und weiterer Überblick zur Vertiefung

Kontakte zu den zentralen Ansprechstellen Cybercrime der Polizei:

BKA (Angriffe auf kritische Infrastrukturen)
T 0611/55-15684 | SO41-NKC@bka-bund.de

Baden-Württemberg
T 0711/5401-2444 | cybercrime@polizei.bwl.de

Bayern
T 089/1212-3300 | zac@polizei.bayern.de

Berlin
T 030/4664-924924 | zac@polizei.berlin.de

Brandenburg
T 03334/388-8600 | cybercrime.fdlka@polizei.brandenburg.de

Bremen
T 0421/362-19820 | k53@polizei.bremen.de

Hamburg
T 040/4286-75401 | zac@polizei.hamburg.de

Hessen
T 0611/83-8377 | zac.hlka@polizei.hessen.de

Mecklenburg-Vorpommern
T 03866/64-4517 | cybercrime.lka@polmv.de

Niedersachsen
T 0511/26262-3804 | zac@lka.polizei.niedersachsen.de

Nordrhein-Westfalen
T 0211/939-4040 | cybercrime.lka@polizei.nrw.de

Rheinland-Pfalz
T 06131/65-64760 | lka.cybercrime@polizei.rlp.de

Saarland
T 0681/962-2448 | cybercrime@polizei.slpol.de

Sachsen
T 0351/855-3461 | zac.lka@polizei.sachsen.de

Sachsen-Anhalt
T 0391/250-2244 | ermittlungen.4c@polizei.sachsen-anhalt.de

Schleswig-Holstein
T 0431/160-4545 | cybercrime@polizei.landsh.de

Thüringen
T 0361/314-1425 | cybercrime.lka@polizei.thueringen.de

Kontakte zu Cybersicherheitsdienstleistern, u. a.:

- BSI - Bundesamt für Sicherheit in der Informationstechnik - Liste der qualifizierten APT-Response-Dienstleister; Stand: 17. Mai 2023, Abruf am 21.07.2023
- Daten- und Informationssicherheit - IHK_DE, Abruf am 21.07.2023

Weitere Hinweise unter:

- Sicherheitskooperation Cybercrime: Sicherheitskooperation Cybercrime | Bitkom e.V., Abruf am 21.07.2023
- BSI – Grundschutz: BSI - IT-Grundschutz (bund.de), Abruf am 21.07.2023
- BSI - Maßnahmenkatalog (bund.de), Abruf am 21.07.2023
- ACS - Maßnahmenkatalog (allianz-fuer-cybersicherheit.de), Abruf am 21.07.2023
- BSI - IT-Notfallkarte (bund.de), Abruf am 21.07.2023
- BMI - Publikationen - Leitfaden Krisenkommunikation (bund.de)
- BSI - BSI-Standard 200-4: Business Continuity Management (bund.de)

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Stephan Ursuleac | T 030 27576-126 | s.ursuleac@bitkom.org
Bereichsleiter Verteidigung & Öffentliche Sicherheit

Layout
Anna Stolz | Bitkom e.V.