DCSO

Whitepaper

Schutz vor Ransomware

Praxisorientierter Leitfaden für Unternehmen

Schutz vor Ransomware
Einführung

Ransomware ist längst kein lästiges IT-Problem mehr – sie zählt mittlerweile zu den gravierendsten digitalen Bedrohungen, denen Unternehmen aller Branchen gegenüberstehen. Schon ein einzelner Angriff kann IT-Systeme und betriebliche Abläufe binnen kürzester Zeit zum Stillstand bringen – mit massiven finanziellen und rechtlichen Folgen. Für Unternehmen beschränkt sich das Risiko dabei nicht allein auf verschlüsselte Daten und die Forderung nach Lösegeldzahlungen. Vielmehr sehen sich Betroffene mit komplexen Folgeproblemen konfrontiert – von Reputationsschäden über drohende Datenschutzverstöße bis hin zu einem langfristigen Vertrauensverlust bei Kunden und Geschäftspartnern.

Vor diesem Hintergrund ist es für Unternehmen essenziell, eine klare Orientierung über notwendige Maßnahmen zu erlangen und die Bedrohungen durch Ransomware systematisch zu reduzieren. Durch das folgende praxisnahe Vorgehen werden alle wesentlichen Dimensionen einer wirksamen Verteidigungsstrategie effektiv gestärkt, von der Risikoerkennung über Schutzmaßnahmen bis hin zur schnellen Reaktion und Wiederherstellung im Ernstfall. Diese umfassende Perspektive soll Unternehmen helfen, dem zunehmenden Druck durch Cyberkriminalität gezielt zu begegnen. Des Weiteren soll es ihre digitale Widerstandsfähigkeit nachhaltig erhöhen.

Checkliste
zur Vorbereitung auf Ransomware-Angriffe

Für die Vorbereitung auf Ransomware-Angriffe benötigen Unternehmen das richtige Rüstzeug – die folgende Checkliste bietet dafür eine Grundlage. Die allgemeinen Handlungsfelder lassen sich je nach Unternehmensgröße, Branche und regulatorischen Anforderungen erweitern. Die DCSO unterstützt sowohl bei der Vorbereitung als auch im Ernstfall mit einer verlässlichen Zusammenarbeit.

Stufe 1
Fundament sichern - Die unverzichtbare Basis

Die folgenden, grundlegenden Maßnahmen sollten in jedem Unternehmen umgesetzt werden – unabhängig von Größe oder Branche – und bilden die Basis für weiterführende Schritte.

1. Systematische Grundlagen

a. Sicherung von vertraglichen Mindestanforderungen für Informationssicherheit und Auditrechten bei kritischen Dienstleistern sowie Durchführung von Kontrollen durch Audits
b. Aufbau eines zentralen und nachhaltig gepflegten Asset-Managements

2. Risikoidentifikation und -Handling

a. Identifikation der „Kronjuwelen“ des Unternehmens, mittels Durchführung von:

I. Business Impact Analyse zur Identifikation kritischer Prozesse
II. Feststellung des Schutzbedarfs für kritische Informationen
III. Identifikation von Abhängigkeiten zwischen Informationen und Prozessen mit IT/OT-Systemen, Personal, Dienstleistern, etc. (Strukturanalyse)

3. Technische Absicherung

a. Einführung risikobasiertes IAM/PAM v.a. in Hinblick auf hoch-privilegierte Accounts
b. Absicherung von Clients durch EDR
c. Prozessgestütztes Patch-Management für „Kronjuwelen“-Systeme und Clients

4. Erkennung von verdächtigen Aktivitäten

a. Zentrales Monitoring mit Fokus auf privilegierte Accounts, Systeme und Funktionen („Kronjuwelen“)
b. Implementierung eines (externen) SOCs bzw. MDR (v.a. für kleinere Unternehmen)

5. Reaktionsmaßnahmen

a. Vertragliche Absicherung durch DFIR-Dienstleister inkl. Prozessverzahnung
b. Erstellung und Testen von Geschäftsfortführungsplänen für kritische Geschäftsprozesse

6. Wiederherstellung

a. Erstellung gehärteter (sicherer) Backups entlang der identifizierten „Kronjuwelen“ (Infrastrukturen)
b. Definition und Testen des kritischen Wiederherstellungspfads

Stufe 2

Verteidigung stärken – Für fortgeschrittene Organisationen

Diese Maßnahmen gehen über das Basisniveau hinaus, bieten zusätzlichen Schutz und sorgen für Prozessreife durch kontinuierliche Verbesserung.

1. Systematische Grundlagen

a. Aufbau eines ISMS (nach ISO 27001)
b. Aufbau eines BCMS (nach ISO 22301)

2. Technische Absicherung

a. Strukturierte Systemhärtung (v.a. für extern erreichbare Hosts und Server)
b. Vollumfängliche Netzwerksegmentierung
c. Zentrales Threat- und Vulnerability-Management

3. Reaktionsmaßnahmen

a. Aufbau eines belastbaren Incident-Response-Frameworks und Information-Security-Incident-Managementsystems
b. Abstimmung von Incident-Response-Maßnahmen mit BCM-Plänen

6. Wiederherstellung

a. Erstellung gehärteter „sicher“ Backups für kritische Applikationen und Services
b. Definition und Testen von Wiederherstellungsplänen für kritische Applikationen und Services

Stufe 3

Strategische Resilienz aufbauen

Diese abschließenden Maßnahmen sorgen für die wechselseitige Verzahnung der verschiedenen Disziplinen und runden den allgemeinen Funktionsumfang ab.

1. Systematische Grundlagen

a. Nutzung von spezialisierten Tools zur ISMS-/BCMS-Dokumentation und Steuerung
b. Aufbau und Handling von Supplier-Management nach ISO 28000
c. Aufbau und Betrieb IRBC-Managementsystem
(ICT Readiness for Business Continuity, nach ISO 27031)

2. Erkennung von verdächtigen Aktivitäten

a. Monitoring externer Bedrohungen (bspw. Darkweb-Monitoring, Leakage-Monitoring)

3. Reaktionsmaßnahmen

a. Aufbau Krisenmanagement inkl. Stakeholdermanagement und Krisenkommunikation
b. Regelmäßige integrierte Übungen und Tests für die gesamte Krisen- und Notfallorganisation

4. Wiederherstellung

a. Verzahnung von Wiederherstellungsstrukturen mit Incident-, Business-Continuity- und Krisenmanagement

Ransomware verstehen

Mehr als nur Datenverschlüsselung

Für einen wirksamen Schutz ist es wichtig zu verstehen, wie Ransomware-Angriffe ablaufen und was auf dem Spiel steht. Typische Angriffe folgen dabei einem strukturierten, oft mehrstufigen Vorgehen: Ein Zeichen dafür, wie stark sich Cyberkriminelle professionalisiert haben.

Ablauf eines Ransomware-Angriffs

Ein Überblick

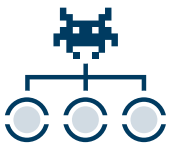
1. Reconnaissance und initialer Zugriff

Cyberkriminelle setzen vor Beginn eines Angriffs typischerweise auf Aufklärung durch Social Engineering oder automatisierte Scans (Reconnaissance), um leichte Ziele und Angriffswege zu identifizieren. Der Angriff beginnt mit der Kompromittierung des ersten Systems im Zielnetzwerk. Dieser Zugriff kann beispielsweise erlangt werden durch:

- Phishing-E-Mails mit schädlichen Anhängen oder Links, Ausnutzung von Schwachstellen in öffentlich erreichbaren Anwendungen (z. B. RDP, VPN, Web-Server), oder
- gestohlene Zugangsdaten, die beispielsweise über das Darknet beschafft wurden.

2. Aufbau und Etablierung der Persistenz

In dieser Phase verschaffen sich Angreifer dauerhaften Zugriff auf das betroffene System. Dabei nutzen sie Backdoors oder spezielle Angreifer-Tools, um auch dann die Kontrolle zu behalten, falls der ursprüngliche Angriffsvektor geschlossen wird.



3. Lateral Movement (Bewegung im Netzwerk)

Anschließend versuchen Angreifer, sich lateral im Netzwerk weiter auszubreiten und möglichst viele Systeme und Nutzerkonten zu übernehmen, insbesondere solche mit hohen Berechtigungen wie etwa Zugänge zum Domain-Controller oder Backup-Server. Dazu nutzen sie Techniken wie:

- Pass-the-Hash bzw. Pass-the-Ticket, Credential Dumping (z. B. mit Mimikatz), oder Remote Code Execution über legitime Admin-Tools (z. B. PowerShell, PsExec).

4. Daten-Exfiltration

Moderne und gut organisierte Ransomware-Gruppen stehlen vor der Verschlüsselung sensible Daten, um damit weiteren Druck auf das angegriffene Unternehmen auszuüben. Dabei drohen die Angreifer mit der Veröffentlichung dieser Daten („Double Extortion“), sofern das Lösegeld nicht gezahlt wird.

5. Verschlüsselung

Die Verschlüsselung erfolgt meist erst, nachdem Angreifer genügend Systeme kontrollieren und relevante Daten extrahiert haben. Ziel ist maximaler Schaden durch eine weitreichende Betriebsunterbrechung. Dazu wird die Ransomware oft gleichzeitig auf mehreren Systemen aktiviert, um Gegenmaßnahmen zu erschweren oder zu verhindern. Typischerweise betroffen sind kritische Systeme wie produktive Applikationen, Clients, Datei- und Datenbankserver sowie ggfs. Backup-Systeme. Nach der Verschlüsselung erhalten die Dateien neue Endungen und die Angreifer hinterlassen Lösegeldforderungen über sogenannte „Ransom Notes“ mit Zahlungsanweisungen in Kryptowährungen.

6. Erpressung und Verhandlung

Angreifer fordern meist Lösegeld, oft in Form von Kryptowährungen wie Bitcoin oder Monero, und stellen ihren Opfern Kontaktinformationen bereit, beispielsweise über ein Portal im Darknet oder einen verschlüsselten Messenger. Um den Druck auf das Opfer gezielt zu erhöhen, drohen sie mit der Veröffentlichung gestohlener Daten (s. 4.: Daten-Exfiltration, „Double Extortion“) und unterbrechen den Betrieb zudem durch (D)DoS-Angriffe („Triple Extortion“). Sollte es zu einer Verhandlung kommen, zeigen sich Angreifer oft kommunikativ und demonstrieren ihre Fähigkeiten zur Datenwiederherstellung.

Auch wenn viele Angriffe nach ähnlichen Mustern ablaufen, gibt es keine Gewissheit für Unternehmen in Bezug auf den Erfolg der Gegenmaßnahmen. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt die Zahl sogenannter Ransomware-as-a-Service-Gruppen weiter zu. Diese Gruppen machen ihre Dienste Kriminellen frei zugänglich und bieten damit auch Akteuren mit wenig technischem Know-how die Möglichkeit, Angriffe durchzuführen. Dadurch steigt die Wahrscheinlichkeit für Angriffe erheblich. Umso wichtiger ist es, wirksame Schutzmaßnahmen zu ergreifen und Angriffe frühzeitig zu erkennen, um Schäden bestmöglich abzuwehren.

Risiko- und Schadensbetrachtung
von Ransomware-Angriffen

Ransomware-Angriffe verursachen im Eintrittsfall erhebliche Schäden. Diese können grob in technische, wirtschaftliche, rechtliche oder strategische Bereiche unterteilt werden und ziehen sowohl kurzfristige als auch langfristige Folgen nach sich.

1. Datenverlust oder eingeschränkte Datenverfügbarkeit

In den meisten Fällen ist das zuerst wahrzunehmende Symptom eines erfolgreichen Ransomware-Angriffs, dass Daten aufgrund der Verschlüsselung nicht verfügbar sind. Bei unzureichenden oder kompromittierten Backups kann für betroffene Unternehmen dabei ein dauerhafter Datenverlust entstehen, wobei auch im Fall von verfügbaren Backups die Daten zumindest temporär nicht zur Verfügung stehen. Resultierend daraus kann es zum Verlust von sensiblen Geschäfts- und Kundendaten oder vertraulichen Forschungsunterlagen kommen. Andererseits können davon abhängige Prozesse wie beispielsweise Buchhaltungs- oder Vertriebsprozesse teils über Wochen hinweg beeinträchtigt sein.

2. Betriebsunterbrechung

Die Verschlüsselung von geschäftskritischen Systemen und Infrastrukturen führt zu einem teilweisen oder sogar vollständigen Stillstand des Betriebs und damit zum Erliegen der gesamten Wertschöpfungskette des Unternehmens. Dadurch ergeben sich Verzögerungen in der Kundenkommunikation und Bearbeitung von Aufträgen sowie Produktionsausfälle infolge von Nichtverfügbarkeit von Produktionssteuerung, die zu Lieferverzögerungen, Umsatzverlusten oder Vertragsstrafen führen können. Dieses Problem wird bei automatisierten bzw. voll digitalisierten und fein aufeinander abgestimmten Prozessen verstärkt, da es kaum noch manuelle Rückfallprozesse gibt. Abseits davon kann eine Betriebsunterbrechung, vor allem im medizinischen Bereich, schwerwiegende Folgen haben, die unter Umständen auch das gesundheitliche Wohl von Patienten bedrohen.

3. Rechtliche und regulatorische Konsequenzen oder Vertragsstrafen

Der Diebstahl von personenbezogenen Daten und die damit verbundene drohende Veröffentlichung dieser Daten können zu empfindlichen Strafen im Rahmen der jeweiligen Datenschutzgesetzgebung führen. Neben diesen möglichen Gesetzesverstößen (z. B. DSGVO in Deutschland) drohen weitere rechtliche Verfahren oder Bußgelder. Insbesondere durch NIS-2 greifen zusätzliche Pflichten, unter anderem Meldepflichten gegenüber zuständigen Behörden, welche eingehalten werden müssen. Als Konsequenz daraus können sich für betroffene Unternehmen im schlimmsten Fall hohe Geldbußen, rechtliche Auseinandersetzungen (und damit verbundene Kosten) und Haftungsansprüche gegenüber Kunden und Vertragspartnern ergeben. Zusätzlich dazu müssen ggf. zusätzliche Audit-Verpflichtungen eingegangen werden.

Weitere Risiken
von Ransomware-Angriffen

Reputationsschäden und Vertrauensverlust

Ein Cyber-Vorfall – insbesondere der Umgang des betroffenen Unternehmens damit – kann das Vertrauen von Kunden, Partnern und Investoren in die Sicherheitsstandards nachhaltig erschüttern. Die Folgen reichen vom Verlust bestehender Kundenbeziehungen über sinkende Marktanteile bis hin zu negativen Auswirkungen auf die zukünftige Kreditwürdigkeit und Geschäftsanbahnung.

Finanzielle Risiken

Neben möglichen Umsatzeinbußen oder Geldstrafen können weitere finanzielle Schäden entstehen, die je nach Unternehmensgröße existenzbedrohend sein können. Die von den Angreifern geforderten Lösegeldsummen, meist in Form von Kryptowährungen, können immens ausfallen. Selbst eine Zahlung bietet keine Garantie für die Wiederherstellung der Daten. Es besteht zudem das Risiko, durch eine Lösegeldzahlung gegen geltende Rechts- oder Compliance-Vorgaben zu verstoßen. Auch für die Wiederherstellung von Systemen ohne Lösegeldzahlung müssen hohe Kosten eingeplant werden, unter anderem für forensische Dienstleistungen, aber auch für die Wiederaufnahme des Betriebs der bestehenden Infrastruktur.

Eingeschränkter Versicherungsschutz

Darüber hinaus ergeben sich weitere mögliche Konsequenzen, sofern das betroffene Unternehmen eine Cyber-Versicherung hat. Bei unzureichender Vorbereitung oder gar Verstößen gegen die in den Policen vereinbarten Maßnahmen zeigen sich Versicherer zurückhaltend bei der Schadensregulierung oder weisen diese ab. Im Fall einer Regulierung muss mit erhöhten Kosten, strengeren Kontrollen oder sogar der Kündigung des bestehenden Vertrags gerechnet werden.

Unternehmen, die von einem Ransomware-Angriff betroffen sind, sehen sich neben diesen materiellen Risiken und Schäden oft auch mit immateriellen Schäden konfrontiert. Dabei sind Beeinträchtigungen in der Unternehmenskultur (z. B. durch Schuldzuweisungen oder Verunsicherung) und die psychische Belastung der Mitarbeitenden (durch Unsicherheit und Angst, dem Verlust des „Sicherheitsgefühls“ oder durch erhebliche Mehrarbeit und Stress) besonders hervorzuheben.

Schritt für Schritt
Wie sich Unternehmen absichern können

Um sich gegen Ransomware abzusichern, benötigen Unternehmen mehr als nur punktuelle Maßnahmen: Tatsächlich ist ein durchgängiges Sicherheitskonzept sehr wichtig. Dabei müssen technische, organisatorische, aber auch menschliche Faktoren berücksichtigt und adressiert werden. Orientierung geben bewährte Rahmenwerke (z. B. ISO-Standards nach Themenfeldern oder NIST Cyber Security Framework) aus der Praxis, denn diese sind international anerkannt und helfen dabei, den Überblick zu bewahren. Das Ziel dieser Rahmenwerke ist es, Sicherheitslücken systematisch zu schließen und im Ernstfall sowohl schnell als auch effektiv reagieren zu können.

Systematische Basis
schaffen

Wirksamer Schutz beginnt mit klaren Strukturen und Verantwortlichkeiten. Es ist wichtig für Unternehmen, dass sie die Maßnahmen nicht nur als Einzelinitiativen begreifen, sondern diese in einem entsprechenden Managementsystem verankern.

Ganz besonders im Kontext von Ransomware müssen die Disziplinen des Informationssicherheits- (ISM) und Business-Continuity-Managements (BCM) im Fokus der Aufmerksamkeit stehen. Es bietet sich demnach an, die internationalen Standards ISO/IEC 27001 (Informationssicherheitsmanagement) und ISO 22301 (Business-Continuity-Management) als Ordnungsrahmen zu verwenden. Damit schaffen Unternehmen die Grundlage für ein systematisches Vorgehen bei der Identifikation, Bewertung und Behandlung von Risiken. Gleichzeitig stiftet dieses Vorgehen Koordination und sorgt für eine kontinuierliche Verbesserung.

Wichtig sind eine durchgängige Dokumentation, Steuerung und Kontrolle – von der Risikobewertung über Maßnahmen bis hin zu Notfalltests, Wirksamkeitsanalysen und Audits. Abhilfe schaffen geeignete ISM- und BCM-Tools, welche über ihre Funktionen und Schnittstellen die Einhaltung von internen und externen Auflagen unterstützen.

Bei der Betrachtung sämtlicher Maßnahmen darf das Ökosystem eines Unternehmens nicht vernachlässigt werden. Auch die Einbindung von Lieferanten, Dienstleistern und Partnern muss systematisch erfolgen. Beispielsweise müssen Sicherheits- und Kontinuitätsanforderungen vertraglich festgelegt werden. Diese Verträge regeln Mindeststandards, Berichtspflichten und die Zusicherung des Rechts zur Auditierung. Als Orientierung kann hierbei auch der ISO 28000-Standard (Supplier-Management) herangezogen werden. Nur durch diese Transparenz und Wahrnehmung der vertraglich zugesicherten Kontrollrechte können Unternehmen die Lieferkette wirksam steuern und Risiken reduzieren.

Risiken
identifizieren

Um sich wirksam gegen Ransomware zu schützen, sollten Unternehmen zwei zentrale Fragen klar beantworten können:

1. **Was ist besonders schützenswert?**
2. **Wo liegen potenzielle Schwachstellen?**

Im Mittelpunkt steht die Identifikation der sogenannten unternehmerischen „Kronjuwelen“ - also jener Informationen, Geschäftsprozesse („Primary Assets“) und zugehörigen Systeme („Supporting Assets“), deren Verlust, Manipulation oder Ausfall besonders schwerwiegende Folgen hätte.

Da diese Analyse vor allem in größeren Unternehmen hinreichend komplex sein kann, gibt es drei zentrale Instrumente, die dafür sorgen, dass der Identifikationsprozess strukturiert und umfassend abläuft:

1. Business-Impact-Analyse (BIA)

Im Rahmen der BIA bewerten Unternehmen für sich, welche Teile der Wertschöpfungskette und damit verbundene Prozesse bei einem Ausfall besonders kritisch sind. Diese Bewertung basiert grundsätzlich auf der Einschätzung der potenziellen Auswirkungen eines Schadens am jeweiligen Prozess. Dabei können Überlegungen zur Aufrechterhaltung der Kundenversorgung, zur Versorgung der regulatorischen Pflichten, zur finanziellen Stabilität sowie zu möglichen Personen- oder Umweltschäden hilfreich sein. Insbesondere bei Ransomware-Angriffen liefert die BIA wertvolle Erkenntnisse über die Prioritäten bei Schutzmaßnahmen und Wiederanlaufstrategien.

2. Schutzbedarfsfeststellung

Aufbauend auf der BIA wird die Schutzbedarfsfeststellung durchgeführt, um Informationen gezielt zu analysieren, welche in den kritischen Prozessen verarbeitet werden. Unternehmen sollten vor allem bewerten, welche Folgen die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit hätte. Die Informationen mit hohem Schutzbedarf (z. B. personenbezogene Daten, geistiges Eigentum oder Finanzdaten) verdienen besondere Aufmerksamkeit, weil diese häufig im Fokus von Angreifern stehen.

3. Strukturanalyse

Bei der Durchführung einer Strukturanalyse machen Unternehmen die Abhängigkeiten zwischen Primärassets (Prozesse und Informationen) und unterstützenden Assets (z. B. Anwendungen, IT-Infrastruktur, Lokationen oder handelnde Personen und Dienstleister) sichtbar. Dadurch wird ersichtlich, welche Komponenten miteinander verbunden sind. Diese Abhängigkeiten machen zentrale Schwachstellen sichtbar und verdeutlichen die potenziellen Auswirkungen eines Ransomware-bedingten Ausfalls entlang der gesamten Prozesskette.

Durch die Kombination dieser Methoden entsteht ein differenziertes, aber konkretes Lagebild, welches als Grundlage für gezielte Schutzmaßnahmen dient. Der Vorteil ist, dass sich Unternehmen hierbei nicht auf Annahmen stützen, sondern fundiert und risikobasiert vorgehen. Weitere Anhaltspunkte zum Vorgehen liefern die Standards ISO/IEC 27005 (Informationssicherheits-Risikomanagement) und ISO 31000 (Risikomanagement).

Ergänzend zu den internen Analysen bringt der gezielte Einsatz von Threat Intelligence wertvolle Impulse bei der Risikoidentifikation. Unternehmen können durch aktuelle Informationen zu Angreifer-Gruppen, deren Taktiken, Techniken und Zielen frühzeitig erkennen, inwiefern sie im Fokus konkreter Bedrohungen stehen (z. B. durch Branchenzugehörigkeit oder eingesetzter Technologien und bekannter Schwachstellen). Damit werden bestehende Analysen geschärft, um Szenarien realistischer bewerten zu können und präventive Maßnahmen gezielt auszurichten. Besonders im Kontext von Ransomware bildet Threat Intelligence ein wichtiges Bindeglied zwischen strategischen Risikobetrachtungen und operativem Schutz.

Auch die systematische Erfassung von (physischen) Geräten und Systemen spielt eine wesentliche Rolle in der Vorbereitung von Maßnahmen gegen Ransomware. Über diese Aufstellung kann durch die Strukturanalyse festgestellt werden, welche Systeme zu priorisieren sind. Dafür ist es essenziell, zu wissen, was konkret im Einsatz ist. Zusätzlich dazu bildet ein gut organisiertes Asset-Management die Grundlage für weiterführende technische Maßnahmen, wie beispielsweise die Reduktion der Angriffsfläche durch die Identifikation von veralteten oder schlecht verwalteten Systemen; beides sind typische Angriffsmarken für Ransomware-Gruppen. Bei entsprechender Verzahnung mit anderen Sicherheitsprozessen bildet das Asset-Management zudem die Grundlage für die Durchgängigkeit von Maßnahmen und Monitoring.

Angriffsfläche reduzieren

Ransomware dringt nicht zufällig in Systeme ein – Angreifer nutzen gezielt Schwachstellen, Fehlkonfigurationen und überhöhte Berechtigungen aus. Daher ist es umso wichtiger, die Angriffsfläche gezielt einzugrenzen und kritische Punkte der Infrastruktur abzusichern. Der Schlüssel liegt hierbei in einer ausgewogenen Kombination aus technischen und prozessualen Maßnahmen, jeweils abgestimmt auf die zuvor identifizierte Risikolage.

Für viele Unternehmen müssen robustes und risikobasiertes Identity- & Access-Management (IAM) und Privilege Account Management (PAM) im Zentrum stehen. Demnach sollten Zugriffsrechte immer nach dem Prinzip der geringstmöglichen Berechtigung (Least Privilege) vergeben und regelmäßig überprüft werden. Vor allem in Microsoft-Infrastrukturen gibt das „Enterprise Access Model“ eine Orientierung hierfür. Die Umsetzung dieses Modells stellt sicher, dass privilegierte Konten strikt von anderen Accounts getrennt sind, mögliche Zugriffspfade reduziert werden und somit die laterale Bewegung (Lateral Movement) sowie unerlaubte Rechteerweiterungen (Privilege Escalation) erschwert werden – ein entscheidender Faktor bei Ransomware-Angriffen.

Ergänzend dazu muss das Unternehmensnetzwerk so segmentiert werden, dass die Verbreitung von Schadsoftware verhindert bzw. größtmöglich erschwert oder verzögert wird. Die granulare Trennung von IT-Umgebungen, etwa zwischen Produktions- und Büronetz oder zwischen administrativen und operativen Bereichen, schafft wichtige Barrieren für Angreifer.

Neben dem Schutz der Identitäten und des Netzwerks ist auch der Schutz von Clients essenziell: Moderne Lösungen (Endpoint Detection & Response) ermöglichen die Erkennung von verdächtigen Aktivitäten und bieten wichtige Funktionen für eine schnelle Reaktion. Dies ist insbesondere dadurch relevant, dass viele Ransomware-Angriffe über kompromittierte Clients eingeleitet werden.

Oft unterschätzt und trotzdem sehr wirksam ist die Systemhärtung, durch welche die Angriffsfläche deutlich reduziert werden kann, insbesondere für die Systeme, die öffentlich erreichbar sind (z. B. über das Internet). Empfehlungen, beispielsweise vom Center for Internet Security (CIS), helfen, Infrastruktur-Komponenten „sicher“ zu konfigurieren und unnötige Funktionen gezielt abzuschalten. Auch wenn diese Maßnahmen grundsätzlich unterbewertet sind, so sind sie ein wertvoller Baustein für eine wirksame Sicherheitsarchitektur.

Zur Handhabe von Schwachstellen bedarf es eines integrierten Threat-, Vulnerability- und Patch-Managements, wobei dies als ein kontinuierlicher Prozess mit definierten Verantwortlichkeiten zu verstehen ist. Die Grundlage dafür bildet ein zentrales Asset-Management. Um zu verhindern, dass bekannte Sicherheitslücken als Einfallstor dienen, sollten Unternehmen auf spezialisierte Tools setzen, welche Schwachstellen frühzeitig erkennen und diese hinsichtlich ihres Risikos bewerten. Als Folge müssen Updates oder alternative Maßnahmen zeitnah und kontrolliert durchgeführt werden.

Schlussendlich stellt diese Auswahl an Maßnahmen nur die wesentlichen und allgemeinen Handlungsfelder dar. Sie können beliebig erweitert werden, beispielsweise durch Konzepte für erweiterte und spezialisierte Infrastrukturen (z. B. Cloud oder OT) oder Applikationen (z. B. SAP).

Wichtig ist, dass die Reduktion der Angriffsfläche nicht als „absolute Sicherheit“ verstanden wird. Vielmehr stellt sie wesentliche Hürden für Angreifer auf und gewinnt damit im Ernstfall wertvolle Zeit zur Reaktion.

Angriffe
frühzeitig erkennen

Je früher ein Ransomware-Angriff erkannt wird, desto größer sind die Chancen, ihn zu stoppen, bevor kritische Systeme betroffen sind. Eine wirksame Erkennung basiert auf einer engmaschigen Überwachung in Form von Logging, Monitoring und Alerting. Hierbei müssen Unternehmen besonderen Fokus auf sehr schützenswerte Bereiche im Unternehmen legen, die „Kronjuwelen“.

Angreifer versuchen gezielt, administrative Konten zu kompromittieren, um so Zugriff auf zentrale Systeme mit weitreichenden Funktionen und Berechtigungen zu erhalten. Daher kommt es nicht nur auf die Überwachung sensibler Daten und Systeme an, sondern auch auf die Aktivitäten privilegierter Accounts. Demnach müssen verdächtige Anmeldeversuche, unzulässige Rechteausweitungen oder ungewöhnliche Zugriffsmuster erkannt und gemeldet werden.

Bei der Überwachung der Infrastruktur müssen Unternehmen besonderen Fokus auf die Systeme legen, die durch privilegierte Identitäten gesteuert werden. Darunter können Clients von Administratoren, Cloud-Konsolen, Sicherheitslösungen oder das interne Netzwerkmanagement fallen. Je nach Branche und Fokus können hier aber auch weitere Komponenten ins Spiel kommen, so z. B. die Steuerungssysteme von Anlagen in der operativen Technologie. In modernen Infrastrukturen zählen diese Systeme zu dem Bereich, der höchst privilegierte Systeme und Funktionen umschließt (vgl. „Tier 0“ bzw. Zugriff auf „Control Planes mittels Privileged Access“, Enterprise Access Model) und damit bei Ransomware-Angriffen häufig Ziel der Eskalation ist. Die lückenlose Überwachung dieser Zonen ist elementar, um Angreifer rechtzeitig zu identifizieren.

Gerade kleine und mittelständische Unternehmen mit kleinen IT-Security-Teams stoßen bei der kontinuierlichen Überwachung schnell an ihre Grenzen. Abhilfe kann ein externes Security Operations Center (SOC) im Rahmen eines „Managed Detection & Response (MDR)“-Services schaffen. Durch den Einbezug eines Dienstleisters werden moderne Analysetools mit erfahrenem Fachpersonal in einem 24/7-Ansatz gebündelt, inklusive direkter Reaktionsmöglichkeiten bei relevanten Vorfällen – vorzugsweise im Schulterschluss mit einem angeschlossenen Incident-Response-Team.

Das Monitoring externer Bedrohungsaktivitäten kann ein hilfreicher Baustein in der Überwachungsstrategie von Unternehmen sein. Dabei werden beispielweise Darknet-Foren oder Leak-Sammlungen durchsucht und überwacht, um gestohlene Zugangsdaten oder gezielte Angriffsplanungen aufzuspüren. Diese Informationen liefern wertvolle Erkenntnisse und können als Frühwarnsignale mitverarbeitet werden.

Grundsätzlich ersetzen Erkennungssysteme keine Schutzmaßnahmen. Sie können jedoch über den Ausgang eines Angriffs entscheiden. Durch die frühzeitige Erkennung von verdächtigen Aktivitäten gewinnen Unternehmen Zeit und erweitern so auch ihren Handlungs- und Reaktionsspielraum.

Schnell
reagieren

Ein Ransomware-Angriff trifft Unternehmen meist ohne Vorwarnung, was dazu führt, dass im Ernstfall jede Minute zählt. Der Unterschied zwischen kontrollierter Eindämmung und unkontrollierbarem Schaden liegt dabei in der Geschwindigkeit und Klarheit der Reaktion. Hierfür werden vorbereitete Strukturen, abgestimmte Rollen und verlässliche Prozesse benötigt.

Im Mittelpunkt steht ein belastbares (Informationssicherheits-)Incident-Response-Framework. Dieses sollte neben der internen Etablierung auch die Zusammenarbeit mit externen Partnern für „Digital Forensics & Incident Response (DFIR)“ umfassen. Durch externe Spezialisten erhalten Unternehmen Zugriff auf Fähigkeiten zur Analyse und Spurensicherung und werden dabei unterstützt, Folgeschäden einzudämmen. Wichtig: Die Zusammenarbeit sollte vertraglich geregelt und regelmäßig erprobt werden, da spontane Vergaben eine schlagkräftige Reaktion nur unnötig verzögern.

Parallel dazu sollten alle zur Verfügung stehenden Reaktionsmaßnahmen mit bestehenden Business-Continuity-Plänen und strategischen Überlegungen abgestimmt sein. Beispielsweise müssen alternative Arbeitsweise bereitstehen, falls zentrale Systeme nicht mehr verfügbar sind. Es braucht also Prozesse zur Umleitung, Ersatzsysteme und unabhängige Kommunikationswege. Im Ernstfall zeigt sich hier, wie gut die technische Sicherheit mit der betrieblichen Widerstandsfähigkeit verzahnt ist. Hilfe bei der Umsetzung liefern die Standards ISO 22301 beziehungsweise ISO 22313 zu Business-Continuity-Managementsystemen.

Neben technischen und operativen Reaktionen benötigen Unternehmen vorbereitete Strukturen für das Krisenmanagement: Es muss geregelt sein, wie die Kommunikation und Handhabe im Ernstfall abläuft – sowohl intern als auch gegenüber Kunden, Partnern, Behörden und Medien. Dazu gehört auch das Stakeholdermanagement, welches bei richtiger Umsetzung in akuten Phasen dabei hilft, Vertrauen zu erhalten und klare Signale zu senden.

In konkretem Bezug auf Ransomware sollten Unternehmen im Vorfeld die Entscheidung treffen, wie sie mit möglichen Lösegeldforderungen umgehen. Hierbei ist es wichtig, Klarheit zu erlangen, ob und unter welchen Bedingungen verhandelt wird. Die Einhaltung von rechtlichen Vorgaben muss unbedingt Teil der Lösungsstrategie sein.

Nicht zu unterschätzen sind die möglichen psychologischen Auswirkungen eines Angriffs, da viele Mitarbeitende in unterschiedlichen Positionen unter großem Druck stehen. Um dem vorzubeugen, können Schulungen, Simulationen oder Krisenübungen helfen, insbesondere in der Führungsriege.

Auch die Reaktionsfähigkeit von Unternehmen profitiert von der Orientierung an bewährten Standards. Bei der strukturierten Bewältigung von Sicherheitsvorfällen empfiehlt sich die Implementierung eines Information-Security-Incident-Management-Systems gemäß ISO/IEC 27035 (alle Teile). Diese Norm bietet einen praxisnahen Rahmen zur Vorbereitung, Erkennung, Analyse und Behandlung (inkl. Nachbereitung) von Vorfällen, auch bei komplexen Bedrohungen wie Ransomware.

Darüber hinaus können auch weitere etablierte Frameworks wie der „NIST Computer Security Incident Handlung Guide (SP 800-61)“ oder das „SANS Incident Handler’s Handbook“ wertvolle Impulse liefern. Dies gilt insbesondere für Unternehmen, die eigene Playbooks oder Reaktionsprozesse (weiter-)entwickeln möchten.

Für das übergeordnete Krisenmanagement auf strategischer Ebene liefert die ISO 22361 hilfreiche Leitfäden, die insbesondere bei großflächigen Ausfällen, öffentlichen Auswirkungen oder Erpressungsszenarien greifen. Mithilfe dieser Orientierung können Unternehmen ihre Führungs- und Kommunikationsprozesse in Krisensituationen strukturieren, indem Rollen klar definiert und Entscheidungswege belastbar gestaltet werden.

Die Reaktionsfähigkeit eines Unternehmens entsteht nicht im Moment des Angriffs, sondern durch eine klare Vorbereitung, regelmäßige Übungen und vorab definierte Entscheidungswege. Nur so lassen sich Fehler vermeiden und Eskalationen kontrollieren, sodass die Auswirkungen eines Angriffs effektiv eingedämmt werden.

Wiederherstellung sicherstellen

Im Ernstfall ist für ein Unternehmen entscheidend, wie schnell es wieder arbeitsfähig wird. Die erfolgreiche Wiederherstellung setzt sorgfältige Vorbereitung, robuste technische Grundlagen sowie eine realistische Einschätzung wesentlicher Abhängigkeiten voraus. Ziel muss es sein, Ausfallzeiten so gering wie möglich zu halten und den Geschäftsbetrieb möglichst reibungslos wieder aufzunehmen – insbesondere bei einem Ransomware-Angriff, bei dem Datenverschlüsselung und damit einhergehender Datenverlust die Regel sind.

Im Zentrum steht die Verfügbarkeit gehärteter Backups für die zuvor identifizierten „Kronjuwelen“, also jener Kombination aus Prozessen, Systemen und Daten, die im Rahmen der Wertschöpfung genutzt oder verarbeitet werden. Diese Backups sollten außerhalb der produktiven Infrastruktur gespeichert und gegen Manipulation geschützt sein. Hilfe leisten hier technische Maßnahmen wie Air Gaps, Immutable Storages und rollenbasierte Zugriffskontrollen. Ebenso wichtig: die regelmäßige und dokumentierte Überprüfung von Backups und zugehörigen Prozessen im Rahmen von Wiederherstellungstests. Nur wenn Backups im Notfall verlässlich funktionieren und verfügbar sind, erfüllen sie ihren Zweck.

Als bewährte Praxis zur Implementierung sicherer Backup-Strategien gilt die 3-2-1-1-0-Regel:

- Drei Kopien der Daten,
- auf zwei unterschiedlichen Medientypen,
- davon eine Kopie an einem externen Ort,
- eine unveränderbare (immutable) Kopie und
- null Fehler bei Wiederherstellungstest.

Ergänzend dazu müssen Unternehmen ihren kritischen Wiederherstellungspfad definieren. Diese Beschreibung gibt an, in welcher Reihenfolge Infrastrukturen, Systeme, Daten und Prozesse wiederhergestellt werden müssen, um einen Mindestbetrieb sicherzustellen. Hierbei müssen wesentliche Abhängigkeiten berücksichtigt werden – etwa, dass Authentifizierungsdienste oder Netzwerkinfrastrukturen zuerst verfügbar sein müssen, bevor spezialisierte Applikationen wieder anlaufen können. Zur Identifikation des Wiederherstellungspfades empfiehlt sich ein schrittweises Vorgehen, bei dem analysiert wird, welche Systeme, Daten und Abhängigkeiten zwingend notwendig sind, um zentrale Geschäftsprozesse wieder aufzunehmen. Idealerweise bilden die zuvor durchgeführten Business-Impact- und Strukturanalysen die Grundlage hierfür. Der definierte Pfad muss regelmäßig getestet und bei technischen Änderungen aktualisiert werden.

Auch für einzelne kritische Systeme (insbesondere für wesentliche Infrastrukturkomponenten) sollten dedizierte Wiederherstellungspläne vorliegen. Dort werden Verantwortlichkeiten, technische Abläufe und Kommunikationswege geregelt und erklärt, welche Unternehmen dabei helfen können, Recovery-Zeiten (Recovery Time Objective, RTO) und Datenverlustgrenzen (Recovery Point Objective, RPO) gegenüber Vorgaben einzuhalten. Auch diese Pläne sollten in realistischen Szenarien erprobt werden, etwa im Rahmen von Tabletop-Übungen oder Recovery-Tests unter Produktionsbedingungen.

Im Notfall, insbesondere bei Ransomware-Vorfällen, ist es wichtig, dass die Wiederherstellung nicht unkontrolliert erfolgt. Dadurch wird die Gefahr reduziert, versehentlich infizierte Systeme oder Schadsoftware erneut einzuschleusen. Aus diesem Grund müssen Recovery-Prozesse eng mit Aktivitäten der Incident Response und Forensik abgestimmt sein, um saubere Ausgangspunkte zu gewährleisten.

Zu guter Letzt: Nach der erfolgreichen Wiederherstellung sollte jeder Vorfall umfassend analysiert und bereits während der laufenden Maßnahmen dokumentiert werden – technisch und organisatorisch. Die gewonnenen Erkenntnisse helfen in der Aufarbeitung des Vorfalls gegenüber Versicherungen, der Staatsanwaltschaft oder Wirtschaftsprüfern und können von Unternehmen genutzt werden, um bestehende Schutzmaßnahmen anzupassen, ihre Prozesse zu verbessern und damit die Resilienz nachhaltig zu stärken.

Fazit

Für Unternehmen bleibt Ransomware eine der größten und dynamischsten Bedrohungen im Bereich der Cyberkriminalität. Hier werden technische Raffinesse und psychologischer Druck so kombiniert, dass die Opfer dort getroffen werden, wo es am meisten schmerzt: bei der Verfügbarkeit zentraler Systeme, dem Vertrauen von Kunden und Partnern sowie der Stabilität der Geschäftsprozesse. Die damit verbundenen Risiken sind vielfältig – vom möglichen finanziellen Schaden über regulatorische und rechtliche Konsequenzen bis hin zu immateriellen Auswirkungen auf Kultur, Moral und Reputation.

Um sich gegen die Bedrohung zu schützen, braucht es mehr als nur technologische Ansätze. Vielmehr ist das interdisziplinäre Zusammenspiel entscheidend: Informationssicherheit, Business Continuity, Krisenmanagement, IT-Betrieb und Führung müssen Hand in Hand arbeiten. Technische Schutzmaßnahmen wie EDR, Segmentierung oder Backup-Härtung sind zwar essenziell, greifen aber nur dann zuverlässig, wenn sie in klare organisatorische und prozessuale Rahmenbedingungen eingebettet sind. Unternehmen, die in diesem Bereich konsequent ihre „Hausaufgaben“ machen, schaffen belastbare Sicherheitsstrukturen.

Ein vollständiger Schutz gegen Ransomware wird nie erreichbar sein, da sich Angriffsstrategien zu schnell und zu professionell weiterentwickeln. Es kann aber sehr wohl dafür gesorgt werden, dass ein erfolgreicher Angriff deutlich erschwert, frühzeitig erkannt und kontrolliert abgewehrt werden kann.

Sicherheit entsteht nicht durch einzelne Maßnahmen, sondern durch eine strukturierte, umfassende und praxisnahe Herangehensweise. Dabei muss der Fokus auf dem Wesentlichen liegen: Risiken verstehen, priorisieren und gezielt reduzieren.

Über die DCSO

Deutsche Cyber-Sicherheitsorganisation GmbH

Seit 2017 steht die Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) für Expertise in der praxisnahen Bekämpfung von Cyberkriminalität. Mit dem Ziel, ein deutsches Kompetenzzentrum zu etablieren, wurde die DCSO von den Gesellschaftern Allianz, BASF, Bayer und Volkswagen gegründet.

Durch eigene Experten, ein umfangreiches Partnernetzwerk und tiefe Einblicke in die Hintergründe und Belange von deutschen Unternehmen bietet die DCSO hochkarätige Dienstleistungen an, welche Kunden dabei helfen, ihre eigene Widerstandsfähigkeit zu erhöhen. Das Leistungsportfolio ist abgestimmt auf große und mittelständische Unternehmen sowie Betreiber kritischer Infrastruktur und enthält:

- Managed Detection & Response
- Digital Forensic & Incident Response
- Threat Intelligence
- Internet Leakage Monitoring
- Beratungsleistungen (technisch und GRC) und Assessments

Darüber hinaus bietet die DCSO einen interaktiven Austausch der Kunden durch eine dedizierte Community.

DCSO
Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin, Germany

+49 30 - 72 62 19 - 0
info@dcso.de

www.dcso.de