Der Weg zu einem integrierten Cyber Incident and Emergency Management

Fallbeispiel „Wie Cyberangriffe deutsche Unternehmen treffen“

White Amflora. Das war der Codename unter welchem die IT-Spezialisten von Thyssenkrupp im Jahr 2016 ihre Systeme dem Zugriff der Winnti Advanced Persistent Threat Gruppe (APT Group G0044)[1] entzogen haben. Der professionelle Cyberangriff begann im Februar desselben Jahres. Entdeckt wurde die Attacke durch das unternehmenseigene Computer Emergency Response Team (CERT). 18 Mitarbeiter und Mitarbeiterinnen, die jeden Tag potenziellen Gefährdungen nachgehen und Alarm schlagen, wenn etwas passiert. Die vollständige Wiederherstellung der Systeme und damit die Beendigung des Angriffs wurde im Oktober 2016 abgeschlossen, acht Monate später[2]. Trotz eines eigenen CERT und einem Heer von IT-Spezialisten. Auch zwischen August und Dezember 2020 wurde die IT verschiedener Sparten von Thyssenkrupp durch drei unterschiedliche Ransomware-Gruppen erfolgreich angegriffen. Dabei wurden verschiedene Informationen, wie Sozialversicherungsnummern, Bankdaten, Gehaltsabrechnungen, oder personenbezogene Daten durch die Angreifer verschlüsselt, zum Teil exfiltriert und im Darknet veröffentlicht[3]. Und ebenfalls im Dezember 2022 meldet Thyssenkrupp erneut, dass Angreifer in die Systeme der Werkstoffsparte Materials Services und Corporate eingedrungen sind. Der virtuelle Einbruch wurde durch die IT jedoch schnell erkannt und die Systeme wieder hergestellt[4].

Sicherlich ist Thyssenkrupp ein prominentes Beispiel und als international tätiger Konzern ein lukratives Ziel für Cyberkriminelle. Auf der anderen Seite sind die Sicherheitsmaßnahmen bei großen Konzernen, und damit die zu überwindenden Hürden, ebenfalls höher. Da Hacker oft den Weg des geringsten Widerstandes suchen, sind auch kleinere und mittelständisch geprägte Unternehmen im Visier der Cyberkriminellen. Dieser Trend wurde 2015 bereits durch die amerikanische Börsenaufsicht festgestellt[5]. Dabei geht es jedoch nicht nur um geringere Sicherheitsvorkehrungen. Viele kleinere und mittelständische Unternehmen sind als Zulieferer oder Dienstleister großer Konzerne oder Behörden auf Landes- und Bundesebene tätig und werden oft als „Sprungbrett“ für Angriffe genutzt[6].

Welche Schäden solche Angriffe anrichten können zeigt das Beispiel des deutschen Fahrradherstellers Prophete. Das Unternehmen mit einer Belegschaft von ca. 450 Mitarbeiter und einem Jahresumsatz in Höhe von 150 Mio. Euro (inkl. Töchter) musste im Dezember 2022 Insolvenz anmelden. Probleme in den Lieferketten und die Verfehlung der geplanten Umsatzziele haben die Insolvenz begünstigt. Der eigentliche Grund liegt laut Insolvenzverwalter jedoch in der mehrwöchigen Betriebsunterbrechung nach einer

[1] https://attack.mitre.org/groups/G0044/
[2] https://www.wiwo.de/my/technologie/digitale-welt/attacke-auf-thyssenkrupp-schon-2016-griff-winnti-an-exklusiver-report-aus-dem-auge-des-sturms/14949912.html
[3] https://securityreport.com/thyssenkrupp-suffers-ransomware-attack-for-the-third-time/
[4] https://www.heise.de/news/Cyberattacke-auf-Thyssenkrupp-7441338.html
[5] https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses#_edn6
[6] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Ransomware-Attacke. Und Prophete ist kein Einzelfall. Laut der amerikanischen Börsenaufsicht wird geschätzt, dass 50% aller kleineren Unternehmen, die Opfer eines Cyber-Angriffs wurden, innerhalb von sechs Monaten nach dem Angriff, ihre Geschäftstätigkeit als Folge dieser Vorfälle einstellen mussten.

Cyber-Angriffe sind damit nicht nur ein lästiges Übel, sondern haben sich zur existenziellen Bedrohung für den Fortbestand von Unternehmen entwickelt. Die zeitnahe Erkennung, eine angemessene Reaktion auf etwaige Vorfälle sowie die Planung dieser Maßnahmen sind folglich für die Sicherstellung der Geschäftstätigkeit unerlässlich.

Einleitung

In unserer modernen und vernetzten Welt genügt es nicht mehr, Cyber-Security als reines IT-Thema zu verorten. Cyber-Security ist ein Thema, das die gesamte Unternehmensorganisation betrifft. Nur ein ganzheitlicher Ansatz, der die organisatorische, technische und standortbezogene Security im Zusammenwirken ihrer Prozesse berücksichtigt, wird erfolgreich sein im Schutz gegen und bei der Abwehr von Cyber-Angriffen. Die richtige Reaktion auf und das richtige Vorgehen bei einem Vorfall sowie die gute Vorbereitung und die Bewältigung des Vorfalls sind Bestandteile einer guten Widerstandskraft (Resilience) der Unternehmen und Institutionen[7]. „Technik allein löst kein Sicherheitsproblem“, da steckt viel Wahrheit drin.

> „Technik allein löst kein Sicherheitsproblem.“

Dieses Positionspapier gibt einen Überblick über bestehende standardisierte Vorgehensweisen zur Prävention und Behandlung von IT-Vorfällen bis hin zur Bewältigung IT-Notfällen geben, die als Folge von Cyber-Risiken entstehen können. Abschließend werden Handlungsempfehlungen abgeleitet, wie die bekannten Vorgehensweisen miteinander verbunden und integriert werden können.

Ziel ist es einen Leitfaden zu erstellen der als Hilfestellung anleitet wie ein integriertes IT-Vorfallsreaktions- und -Bewältigungsmanagement umgesetzt werden kann, um die Resilienz der Unternehmen und Institutionen gegen Bedrohungen aus dem Cyberraum zu erhöhen.

Daher werden zunächst die aktuellen Herausforderungen im Umfeld der Cyber-Security dargestellt. Daran anschließend werden aus dem Security Incident Management (SIM), IT-Notfall- bzw. IT-Service Continuity Management (ITSCM) und Business Continuity Management (BCM) bekannte Vorgehensweisen beschrieben.

Herausforderungen der weltweiten digitalen Vernetzung

Motivation der Angreifer

Die Bedrohung für Unternehmen, durch Cyber-Angriffe auf ihre Infrastruktur Schaden zu erleiden, ist in den letzten Jahren stetig angestiegen und wird voraussichtlich auch 2023 und 2024 im zweistelligen Prozentbereich wachsen, nachdem von 2021 auf 2022 bereits eine Zunahme der wöchentlich registrierten Cyberattacken von 38% zu verzeichnen war. Das Spektrum der Angreifer ist groß und zieht sich von den privaten Hackern mit unterschiedlicher Motivation über befähigte Einzeltäter und organisierte, kriminelle Strukturen bis hin zu spezialisierten Hacker-Gruppen, die aus monetärer oder politischer Motivation heraus agieren. Letztere sind mitunter überaus professionell, mit hoher Wirkung aktiv und greifen gezielt Unternehmen sowie staatliche Strukturen an. Es steckt nicht immer die Geldgier krimineller Hacker dahinter, sondern zunehmend auch das Interesse daran, Unternehmen mit hohem Anteil an der Wirtschaftskraft eines Staates oder ganze Regionen / Staaten gezielt zu destabilisieren.

[7] Siehe Leitfaden Cyber-Sicherheits-Check Version 2 Maßnahmenziel H Bewältigung von Sicherheitsvorfällen/Notfällen https://isaca.de/publikationen/publikationen/leitfaeden/cyber-sicherheits-check-version-2.html

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Die größten Bedrohungen sind dabei die Ransomware-Angriffe gefolgt von DDoS-Angriffen. Folge dieser Angriffe sind Störungen des Geschäftsbetriebs bis hin zum Ausfall kritischer Unternehmensprozesse, Datenschutzverstöße und Verlust von kritischen Unternehmensdaten oder, wie im obigen Beispiel dargestellt, bis hin zur Insolvenz.

Laut dem Threat Landscape for Ransomeware Attacks der European Network and Information Security Agency (ENISA) werden durchschnittlich 10 Terrabyte an Daten pro Monat gestohlen. Die Untersuchungen zeigen, dass 58,2 % der gestohlenen Daten persönliche Daten von Mitarbeitern enthalten. Bei 94,2% der Vorfälle ist nicht bekannt, ob das Unternehmen das Lösegeld gezahlt hat oder nicht. Bei 37,88% der Vorfälle wurden jedoch Daten auf den Webseiten der Angreifer veröffentlicht, was darauf hindeutet, dass die Lösegeldverhandlungen gescheitert sind. Hieraus kann angenommen werden, dass 62,12% der Unternehmen sich möglicherweise auf eine Vereinbarung bezüglich der Lösegeldforderung eingelassen haben[8].

Motivation der Unternehmen

Kaum ein Unternehmen kommt heutzutage noch ohne IT aus. Wie groß die Abhängigkeit der geschäftskritischen Prozesse von einer funktionierende IT allerdings wirklich ist, stellen viele Unternehmen erst fest, sobald es zu spät ist. Physische Zutrittsbeschränkungen oder Vorkehrungen im Brandfall zählen heutzutage, auch durch regulatorische Vorgaben, zum Standardrepertoire. In gleicher Weise sollten sich Unternehmen auch auf Angriffe aus dem Cyber-Raum vorbereiten. Und da es – getreu dem Motto "Es ist nicht die Frage 'ob', sondern 'wann'" – keine 100-prozentige Sicherheit gibt, gilt es Maßnahmen zur Behandlung von Sicherheitsvorfällen vorzubereiten. Dies beginnt mit der formalen, theoretischen Beschreibung, wie im Ernstfall zu reagieren ist und endet mit regelmäßigen Trainings. Strapaziös ist ein Sicherheitsvorfall in jedem Fall. Je besser man vorbereitet ist, umso schneller und effizienter lassen sich der Vorfall beheben und damit größere Schäden wie Umsatzausfälle oder Datenverluste einschränken oder ganz verhindern. Aufgrund der weltweiten Vernetzung ist dies also nicht mehr ein reines Compliance-Thema für große Unternehmen, sondern sollte im Eigeninteresse eines jeden Mittelständlers und Kleinstunternehmens umgesetzt werden.

Übersicht der Managementsysteme zur Betriebskontinuität

Information Security Incident Management

Das Information Security Incident Management (ISIM) ist ein Prozess des Information Security Management Systems (ISMS), bspw. nach ISO/IEC 27001[9]. Das ISIM wird im Umsetzungsleitfaden der ISO/IEC 27035 beschrieben. Weitere Umsetzungsleitfäden wie z.B. die ISO/IEC 27037 Digital Forensic vervollständigen die Vorgehensweisen. Heute fasst man das unter Digital Forensic and Incident Response (DFIR) zusammen.

DFIR ist somit ein fester Bestandteil des Information Security Incident Management im ISMS. Es ist ein Vorgehensmodell für die Behandlung von Cyber-Incidents. In Abb. 2 wird der Incident Response Prozess nach NIST SP 800-61 visualisiert das den Teil Incident Responce des DFIR noch weiter detailliert. Die einzelnen Schritte werden nachfolgend kurz erläutert.

[8] ENISA Threat Landscape for Ransomware Attacks July 29, 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
[9] https://isaca.de/publikationen/publikationen/leitfaeden/implementierungsleitfaden-iso-iec-27001-2022.html

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

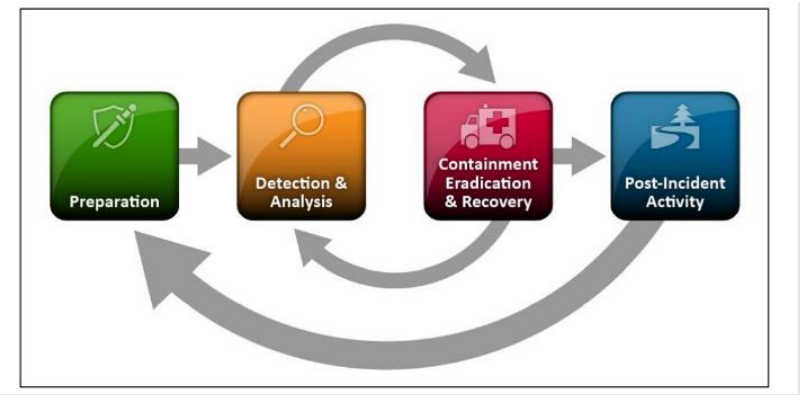

Abbildung 23: Incident Response Life Cycle, Quelle: NIST SP 800-61

Preparation

In diesem Schritt werden Pläne entwickelt, um auf mögliche Vorfälle vorbereitet zu sein. Es werden Tools und Prozesse etabliert, um angemessen auf einen Vorfall reagieren zu können. Dazu gehört u.a. auch die regelmäßige Schulung der Mitarbeiter, um sicherzustellen, dass sie im Falle eines Vorfalls wissen, was zu tun ist. Eine gute Vorbereitung kann dazu beitragen, den Schaden zu minimieren und den normalen Geschäftsbetrieb so schnell wie möglich wieder aufzunehmen.

Detection

Um zu wissen, wann ein Security Incident eintritt, ist es wichtig in der Detection Angriffe rechtzeitig zu erkennen. Ziel der Detection ist es, mögliche Anzeichen für einen Vorfall zu identifizieren (bspw. durch Indicator of Compromise, IoC). Dazu können u.a. ungewöhnliche Netzwerkaktivitäten, auffällige Zugriffsversuche oder andere Verhaltensmuster gehören, die auf eine Sicherheitsbedrohung hinweisen. Die Erkennung sollte durch automatisierte Prozesse unterstützt und durch manuelle Prüfungen ergänzt durchgeführt werden, um sicherzustellen, dass alle relevanten Bedrohungen identifiziert werden.

Analyse

Wurde ein möglicher Angriff erkannt, ist der Alarm in der Analysis als true-positive oder false-positive einzustufen. Dazu werden systemseitig generierte Informationen wie bspw. Security Events (Logs) analysiert und schließlich eine Klassifizierung des Vorfalls vorgenommen. Die Klassifizierung sollte auf der Basis einer Bewertung der Bedrohung, des potenziellen Schadens und der Schwere des Vorfalls erfolgen. Dies hilft bei der Entscheidung, welche Ressourcen zur Bewältigung des Vorfalls benötigt werden. Sobald der Vorfall als relevant eingestuft wurde, sollte er an das Incident-Response-Team und/oder Digital-Forensics-Team weitergeleitet werden. Die Eskalation kann auch die Kommunikation mit Mitarbeitern, anderen Abteilungen, Auftragnehmern oder Behörden umfassen. Auf diese Weise ist sicherzustellen, dass alle notwendigen Schritte unternommen werden, um den Vorfall zu bewältigen und ggf. strafrechtlich relevante Beweise zu sichern.

Containment

Handelt es sich um einen true-positive Vorfall, so startet das Containment. Um eine Ausweitung des Schadens zu begrenzen und dadurch den Umfang und Dauer eventueller Ausfälle zu reduzieren, wird im Rahmen des Containments ein aufgetretener Vorfall eingedämmt. Dies beinhaltet mitunter unliebsame Maßnahmen, wie die partielle Abschaltung von Systemen, die Trennung von Netzwerkverbindungen oder die Deaktivierung einzelner Services. Da zuvor genannte Entscheidungen mitunter weitreichende Konsequenzen für den Geschäftsbetrieb haben, sollten diese bereits geplant und auch im BCM berücksichtigt werden, damit im Bedarfsfall die rechtzeitige Eindämmung eines Vorfalls nicht an fehlenden Entscheidungen scheitert.. Entsprechende Eindämmungsstrategien ermöglichen es dem Incident-Response-Team angemessen auf die Situation zu reagieren, ohne wertvolle Zeit verstreichen zu lassen und hierdurch das Ausmaß des Vorfalls unnötig zu erhöhen. Eine Eindämmung des Vorfalls ermöglicht es dem

Incident-Response-Team, die Situation zu bewerten und Gegenmaßnahmen einzuleiten, was die nächste Phase des Information Security Incident-Management-Prozesses einleitet.

Eradicate

Konnte die weitere Ausbreitung eingeschränkt werden, so wird mit der Eradication begonnen. Die Beseitigung bzw. Behebung der Ursache eines Vorfalls, im Rahmen eines Information Security Incidents meistens verbunden mit der Bereinigung betroffener Systeme, ist die Tätigkeit, mit welcher der Begriff Incident Management am ehesten verbunden wird. Hierbei gilt es, die Ursache zu suchen, diese zu analysieren, um sie zu beseitigen, und ein erneutes Kompromittieren vermeiden zu können. Ein wichtiger Aspekt ist es hierbei, eine rechtssichere Beweisführung zu ermöglichen und eine umfassende Dokumentation anzufertigen. Nicht nur, um die Aufarbeitung und spätere Auswertung zu ermöglichen, sondern auch um diese ggf. in einem Gerichtsverfahren als Beweise nutzen zu können. Sind die Ursache und das Ausmaß des Vorfalls geklärt und, im Falle eines Security Incidents, angemessene Beweise sichergestellt, müssen die betroffenen Systeme bereinigt werden. Das beinhaltet u.a. das Einspielen von Datensicherungen, um Datenschiefstände oder verfälschte Informationen zu entfernen, die Löschung von installierter Schadsoftware und Backdoors, Deaktivierung von kompromittierten Benutzeraccounts bzw. Löschung von Angreifern neu erstellten Accounts, Prüfung und Bereinigung von Berechtigungsstrukturen, Gruppenrichtlinienobjekten wie auch Registrierungsschlüsseln. Auch die bei der Analyse gefundenen Sicherheitslücken sind ebenfalls im Rahmen der Bereinigung zu schließen. Wichtig ist, dass alle betroffenen Systeme identifiziert, von der produktiven Umgebung getrennt und bereinigt werden, da sonst eine erneute Kompromittierung droht.

Recovery

Nach der Bereinigung kann im Rahmen des Recovery mit der Reintegration der gereinigten Systeme in die Produktionsumgebung begonnen werde und somit den Nutzern wieder zugänglich gemacht werden. Die Wiederinbetriebnahme sollte mit einer Hyper-Care-Phase verbunden werden, welche eine intensive Überwachung der betroffenen Systeme umfasst. Ein einmal befallenes System wird, auch durch die gewonnenen Erkenntnisse über das IT-System, oft zum erneuten Ziel von Angreifern. Systeme mit ähnlichen Funktionen sollten ebenfalls verstärkt detektiert werden.

Post Incident Activity

Schließlich ist der Vorfall mit einer Post-Incident Activity abzuschließen. Sind der Vorfall behoben, die Systeme bereinigt und der Normalbetrieb wieder angelaufen, sollten die gewonnen Erkenntnisse aufgearbeitet werden, um die Wahrscheinlichkeit für die Wiederholung des Zwischenfalls zu reduzieren und den Prozess des Incident Managements zu verbessern. Ein Lessons-Learned-Meeting als wichtiger Bestandteil eines kontinuierlichen Verbesserungsprozesses wird im Incident Management oft vernachlässigt. Dabei geht es nicht nur darum, zu verstehen, was genau passiert ist, sondern zu evaluieren, ob der Information Security Incident-Management-Prozess als solcher angemessen funktioniert hat oder Anpassungen vorzunehmen sind.

Business Continuity Management

Beim Business Continuity Management (BCM) handelt es sich um ein Managementsystem zur Sicherstellung der Aufrechterhaltung oder zeitnahen Wiederherstellung zeitkritischer Geschäftsprozesse und Lieferketten, sofern diese durch wesentliche interne oder externe Ereignisse unterbrochen wurden. Im Rahmen eines BCM wird die Kritikalität betrieblicher Prozesse ermittelt, ebenso die validen Bedrohungsszenarien und die daraus resultierenden Risiken. Anschließend werden Maßnahmen festgelegt und umgesetzt, um die Auswirkungen eines Vorfalls zu mitigieren und den daraus entstehenden Schaden zu minimieren. Der Fokus liegt dabei auf der Aufrechterhaltung der geschäftskritischen Betriebsprozesse im Schadenfall. Dabei kann der Betrieb, je nach eingetretenen Schadensereignis, auch reduziert bzw. zeitlich begrenzt eingeschränkt im Notbetrieb weitergeführt werden. Wichtigstes Instrument für die Erhebung und Ermittlung der geschäftskritischen Prozesse ist die Business Impact Analyse (BIA), bei der die Verfügbarkeitsanforderungen aus prozessualer Sicht bewertet und die notwendigen Ressourcen für den

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Normal- und den Notbetrieb aufgenommen werden. Die BIA ermöglicht es, die Geschäfts- sowie Unterstützungsprozesse hinsichtlich ihrer Kritikalität zu ordnen, um so die begrenzten Ressourcen im Katastrophenfall optimal einzusetzen. Um eine umfassende Bewertung der Risiken sowie betrieblichen Belange vornehmen zu können, sollte der BCM-Prozess Vertreter aus jedem Fachbereich miteinbeziehen und sich nicht auf den IT-Bereich beschränken, was den wesentlichen Unterschied zum IT-Notfallmanagement darstellt.

Das primäre Ziel des BCM ist es, die finanziellen, rechtlichen und reputationsschädigenden Folgen einer Betriebsunterbrechung zu minimieren.

Im Kontext dieses Positionspapiers spielt das BCM als organisationsweites Managementsystem eine wesentliche Rolle, da ein Teil seiner Prozesse und Prozeduren den Security-Incident-Management Prozess wie auch den Prozess der IT-Notfallplanung (IT-Service Continuity Management) wesentlich unterstützen.

IT-Notfallmanagement

Das IT-Notfallmanagement (ITSCM) kann als Bestandteil des Business Continuity Management (BCM) verstanden werden, spezialisiert auf die Belange der IT-Organisation. Die meisten Unternehmen sind bei der Durchführung ihres Tagesgeschäfts stark auf IT-Services angewiesen. Das IT-Notfallmanagement dient dem Zweck, den IT-Betrieb auch bei einem Ausfall wesentlicher IT-Ressourcen schnellstmöglich wiederherstellen zu können und IT-Notfälle beherrschbar zu machen. Daraus ergeben sich die folgenden zentralen Ziele des IT-Notfallmanagements:

- Die Wiederherstellbarkeit der zentralen IT-Systeme muss auch bei Eintreten eines Notfalls sichergestellt werden. Daher werden effiziente und zielgerichtete Methoden, Verfahren und Hilfsmittel zur Notfallvorsorge und -bewältigung entwickelt.
- Die Reputation des Unternehmens darf in der Öffentlichkeit nicht durch fehlende Notfallvorsorge und/oder mangelhafte Notfallbewältigung im Bereich der IT beeinträchtigt werden.
- Der Schutz von Mitarbeitern, Geschäftspartnern und Endkunden muss auch im Rahmen von IT-Notfällen jederzeit sichergestellt sein.

Die erforderlichen Prozesse, Strukturen und Rahmenbedingungen zur Sicherstellung der Verfügbarkeit und Kontinuität kritischer IT-Services werden im Rahmen des IT-Notfallmanagements entwickelt. Es umfasst die Identifizierung potenzieller Risiken für IT-Dienste, die Bewertung ihrer Auswirkungen und die Umsetzung von Strategien zur Risikominderung und Aufrechterhaltung des IT-Betriebs.

Falls aufgrund eines Notfalls die benötigten IT-Ressourcen nicht mehr zur Verfügung stehen, kann der Geschäftsablauf und damit nicht zuletzt die Erreichung der Unternehmensziele gefährdet werden. Aus diesem Grund ist eine hinreichend qualifizierte Vorsorge für alle relevanten Szenarien zu treffen, sodass ein eingetretener Schaden schnell und systematisch begrenzt und behoben werden kann. Um das zu erreichen, benötigt die IT ein effektives und kosteneffizientes Notfallmanagement, das idealerweise in Form eines ganzheitlichen Managementprozesses umgesetzt wird. Dieser Prozess sollte durch entsprechende Dokumentation definiert sein und die in Abb. 1 dargestellten Aktivitäten beinhalten.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

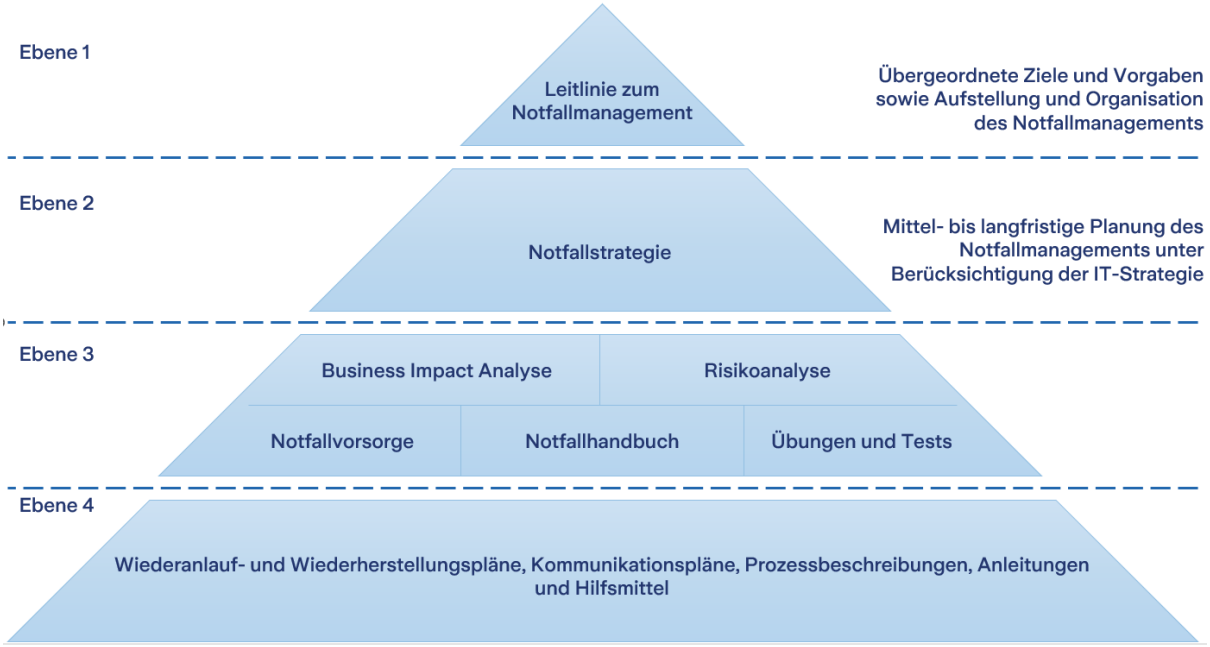

Abbildung 1: Aufbau des ganzheitlichen Notfallmanagementprozesses (eigene Darstellung)

Das IT-Notfallmanagement fokussiert die Anforderungen des BCM an die IT-Services. Die in der Business Impact Analyse (BIA) definierten Anforderungen an die Verfügbarkeit geschäftskritischer Anwendungen werden aus dem BCM an das IT-Notfallmanagement weitergegeben. Dort werden die Verfügbarkeitsanforderungen aus der BIA mit dem aktuellen Stand der IT-Betriebsstabilität im Rahmen einer Gap-Analyse verglichen. Die hierbei identifizierten Lücken gilt es durch angemessene Planung, Design und Implementierung von Maßnahmen zu schließen.

Aktivitäten wie bspw. die Analyse der Auswirkungen auf das Geschäft, die Risikobewertung sowie die Entwicklung von Wiederherstellungsstrategien werden vom BCM koordiniert und durchgeführt. Bei der Analyse der Auswirkungen auf das Geschäft werden die potenziellen Auswirkungen schwerwiegender Ausfälle auf kritische IT-Dienste und das Unternehmen als Ganzes bewertet. Bei der anschließenden Risikobewertung geht es um die Ermittlung potenzieller Bedrohungen für IT-Service, wie Naturkatastrophen, menschliches Versagen oder die insbesondere hier thematisierten Cyber-Angriffe. Die sich daran anschließende Ableitung der IT-Notfallvorsorge, Prüfung und Pflege der IT-Notfallpläne sowie Durchführung von Übungen und Tests obliegt dem IT-Notfallmanagement.

Sobald die Risiken und Auswirkungen ermittelt wurden und Wiederherstellungsstrategien entwickelt sind, können konkrete Wiederanlauf- und Wiederherstellungspläne sowie Kommunikationspläne erstellt werden, um die Kontinuität der IT-Service zu gewährleisten. Dies kann die (ggf. zusätzliche) Implementierung von redundanten Systemen, Datensicherungen und alternativen Kommunikationskanälen beinhalten. Die Prüfung und Pflege von Übungs- und Testszenarien sowie regelmäßige Durchführung von Notfalltrainings und -tests sind ebenfalls von entscheidender Bedeutung, um die Aktualität und Wirksamkeit fortlaufend sicherzustellen.

Das primäre Ziel des IT-Notfallmanagements ist, die Kontinuität der IT-Services aufrechtzuerhalten und die Auswirkungen wesentlicher Vorfälle auf das geringstmögliche Maß zu begrenzen. Es handelt sich also um einen entscheidenden Baustein für Unternehmen zur Sicherstellung der geschäftlichen Kontinuität, die im Rahmen des BCM abgesichert wird.

Aktuelle Problemstellung im Zusammenwirken der Managementsysteme

Der Aufbau eines effektiven Managements zur Handhabung von IT-Sicherheitsvorfällen ist für eine Organisation essenziell. Die Bedrohungslage ist akut und betrifft nicht nur Angriffe auf die IT, sondern auch zunehmend die Operative Technologie (OT). Angreifer nutzen dabei sowohl technische als auch organisatorische Schwachstellen aus. Man kann sich nicht zu 100% vor derartigen Angriffen schützen, denn es gibt zu viele Einflussfaktoren, wie z.B. Zero-Day-Exploits, Softwarefehler, unzureichendes Patchmanagement und menschliches Fehlverhalten. Eine Organisation muss daher ein effektives Management zur Handhabung von Sicherheitsvorfällen aufbauen und stetig weiterentwickeln.

Die bekannten Managementsysteme, wie das BCM, IT-Notfallmanagement und Information-Security-Incident-Management sind auf sich allein gestellt kein effektives Mittel zur modernen Vorfallsbekämpfung, aber sie beinhalten die Bausteine ein solches aufzubauen.

- Das Business Continuity Management (BCM) befasst sich mit der Aufrechterhaltung des Geschäftsbetriebes. Es ist nicht fokussiert auf Cyber Angriffe und kann diese in ihrer Komplexität nicht abbilden.
- Das ITSCM oder IT- Notfallmanagement befasst sich mit der Aufrechterhaltung der IT- Services. Es ist in der Lage mit Cyber Angriffen umzugehen, beschränkt sich jedoch auf die IT-Organisation.
- Das Information Security Incident Management (ISIM) befasst sich mit der Vorfallbekämpfung von Cyber Angriffen. Es ist fokussiert auf DFIR, stellt aber keine geeigneten Schnittstellen und Möglichkeiten bereit, es in die ITSCM und BCM- Prozesse zu integrieren.

So ist jedes der benannten Systeme nur teilweise geeignet, Cyber Angriffe effektiv und umfassend zu managen.

Oft fehlen organisatorische Zuständigkeiten, Verantwortlichkeiten sind nicht ausreichend definiert, die IT-Organisation ist nicht auf solche Szenarien vorbereitet, es herrscht Unklarheit über die Prioritäten bei Prozessen und Services, die existierenden Prozesse und Prozeduren zur Vorfallbekämpfung sind nur unzureichend oder gar nicht aufeinander abgestimmt.

Bislang werden z.B. DFIR- Teams im Einsatzfall oft zusätzlich mit Aufgaben konfrontiert, die nicht zu ihren Kernaktivitäten gehören, wie z.B. Verhandlungsführung, Krisenkommunikation, Unterstützung der IT- Organisation bei der Umsetzung von technischen Sofortmaßnahmen.

Wichtige Zeit geht verloren, Entscheidungen werden falsch oder nicht getroffen, technische Sofortmaßnahmen sind nicht vorbereitet, sondern werden improvisiert, Ansprechpartner sind nicht erreichbar, kurzum es fehlt an vielem, es wird schnell unübersichtlich, der Druck ist immens und es treten vermehrt Fehler auf, die durch eine vorausschauende Planung und Vorbereitung vermeidbar gewesen wären.

Unser Lösungsvorschlag

Unser Ziel ist es, einen Leitfaden zum Aufbau eines integrierten Cyber Incident and Emergency Management zu erstellen, welches die Organisation in die Lage versetzt es in die ITSCM- und BCM-Prozesse zu integrieren, um auf dynamisch verändernde Angriffsszenarien angemessen reagieren zu können und handlungsfähig zu bleiben.

Die dafür notwendigen Inhalte und Strukturen wollen wir unter Verwendung bewährter Vorgehensweisen und Methoden aus den zuvor beschriebenen Managementsystemen entsprechend dem nachfolgend aufgeführten Aufbau entwickeln.

Wir orientieren uns hierbei am Prozessmodell des BSI 200-4 in Kombination mit dem Incident-Response-Prozess nach NIST SP 800-61. Ergänzt wird diese Kombination durch weitere Prozeduren aus dem Business-Continuity-Management gemäß ISO/IEC 22301 und weiteren Best Practices, die wir in eine neue Methodik, das Cyber Incident and Emergency Management überführen und hierzu neu strukturieren sowie kombinieren.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Die dazu durchzuführenden Aktivitäten stellen wir grob in den folgenden Schritten dar, die wir in einem Leitfaden detailliert ausarbeiten:

Vorbereitung

- Informationen sammeln: Was ist vorhanden (BCM, ITSCM, Information Security Incident Management, Problem Management, Change-Management)

Ist-Analyse

- Assessment zur Reifegradermittlung (SPICE, CMMI) der notwendigen Prozesse (BCM, ITSCM, Security Incident Management, Problem Management, Change-Management)

Soll-Definition

- Ziele definieren (Organisation, Prozesse, Prozeduren)
- Threat Modelling ITO (MITRE ATT@CK, IRC)
- Schnittstellen identifizieren (BCM, Security Incident Management, Problem Management, Change-Management), (Organisation, Prozesse, Prozeduren)

Umsetzung planen

- Maßnahmen definieren
- Maßnahmen auswählen

Umsetzen

- Maßnahmen umsetzten
- Umsetzung überprüfen
- Umsetzung freigeben

Dokumentieren

- Policies & Procedures

Prüfen und verbessern

- Tests und Übungen
- Prozessaudits
- Organisatorische Audits

Mit diesem Lösungsansatz helfen wir Organisationen dabei, auf Cyber-Angriffe proaktiv reagieren zu können, um dadurch Schaden zu minimieren oder ihn gar nicht erst entstehen zu lassen.

Die Schotten gehen halt nie bis an die Decke und Technik allein löst kein Sicherheitsproblem, was bedeutet, dass allein technische Maßnahmen keinen umfänglichen Schutz bieten, wenn man die organisatorischen Maßnahmen vernachlässigt. Ein pragmatischer, den potenziellen Angriffsszenarien folgender umfassender Ansatz ist aus unserer Sicht ein Weg, um sich besser gegen Cyber-Angriffe aufzustellen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Autorenteam

- Volker Reers
- Alexander Biehl
- Dennis Grebe
- Dirk Schugardt
- Gregor Wittkowski
- Alexander Röttcher
- Detlef Hösterey

Vorstand

- Dr. Tim Sattler (Präsident)
- Thomas O. Englerth (Vizepräsident – Zertifizierungen)
- Dirk Meissner (Vizepräsident – Finanzen und Verwaltung)
- Markus Gaulke (Vizepräsident – Weiterbildung)
- Prof. Dr. Matthias Goeken (Vizepräsident – Veröffentlichungen)
- Julia Hermann (Vizepräsidentin – Kommunikation und Marketing)
- Matthias Kraft (Vizepräsident – Fachgruppen)

Möchten Sie zu diesem Positionspapier mit uns Kontakt aufnehmen. Dann schreiben Sie uns bitte an: FG-cybersecurity@isaca.de

Interessieren Sie sich für weitere Veröffentlichungen des ISACA Germany Chapter? Dann besuchen Sie uns jetzt auf: https://www.isaca.de/de/veroeffentlichungen-des-isaca-germany-chapters