Notfallvorsorge mit internationalen Standards

Die Standards von NIST und ISO/IEC im Bereich der Notfallvorsorge werden weltweit zur Planung der Reaktion auf Sicherheitsvorfälle eingesetzt. Die Hauptempfehlungen der Standards können Unternehmen dabei unterstützen, ihre eigene Reaktionsplanung aufzubauen oder zu verbessern.

Von Jan Huck

Ausführliche Empfehlungen zur Reaktion auf Sicherheitsvorfälle wie die der US-Behörde NIST oder der ISO/IEC können aufgrund der mit Text überladenen Seiten schnell abschreckend wirken. Wen die Fülle an Informationen noch nicht von einer Lektüre abhält, der muss sich durch schwer verständliche Formulierungen kämpfen. Außerdem sind die Empfehlungen so geschrieben, dass sie für Firmen aller Größen, von kleinen Betrieben bis hin zu international agierenden Großunternehmen, gelten, was das Ganze weiter verkompliziert.

Jedoch enthalten diese Empfehlungen viele wertvolle, von Experten zusammengetragene Informationen, die besonders für diejenigen ungemein nützlich sind, die sich zum ersten Mal mit dem Thema befassen. Sie können dazu beitragen, dass alle Aspekte der Reaktion auf Sicherheitsvorfälle bereits bei der Vorbereitung berücksichtigt werden und somit von Anfang an ein robuster Reaktionsplan vorhanden ist. Auch für das Überprüfen der Vollständigkeit eines schon bestehenden Reaktionsplans können die Empfehlungen hilfreich sein. Insgesamt kann ein strukturierter, umfassender Reaktionsplan sicherstellen, dass alle beteiligten Mitarbeitenden im Notfall wissen, wie sie handeln müssen. Im besten Fall können so Maßnahmen frühzeitig eingeleitet werden, um Sicherheitsvorfälle von Anfang an einzudämmen und die negativen Auswirkungen und die Kosten zu reduzieren.

Bekannte Standards für Sicherheitsvorfälle

Die wohl bekanntesten Standards für die Reaktion auf Sicherheitsvorfälle wurden vom NIST (Nationales Institut für Standards und Technologie) und der ISO/IEC (Internationale Organisation für Normung und Internationale Elektrotechnische Kommission) entwickelt. Das NIST veröffentlichte 2012 den überarbeiteten „Leitfaden für den Umgang mit Computersicherheitsvorfällen“ SP 800-61, um amerikanische Behörden bei der Erfüllung ihrer gesetzlichen Pflichten zur Reaktionsplanung zu unterstützen.

Dieser Standard enthält weitreichende Empfehlungen, die auch für Privatunternehmen relevant sind. Auch nach einigen Jahren ist er noch immer aktuell und findet weltweit breite Anwendung bei Firmen aller Größen. Die nicht staatlichen Organisationen ISO und IEC veröffentlichten gemeinsam die ISO/IEC-27035-Reihe „Management von Informationssicherheitsvorfällen“.

Diese Reihe gibt Hilfestellung bei der Implementierung von Maßnahmen aus dem ISO/IEC-27001-Standard, die die Reaktion auf Sicherheitsvorfälle betreffen. Die ISO/IEC 27035-Reihe besteht aus drei Teilen, weitere sind in Planung. Der erste Teil beinhaltet die Grundlagen und den Prozess der Reaktion, während sich der zweite und dritte Teil auf unterschiedliche Phasen des Reaktionsprozesses konzentrieren (alle erwähnten Standards und weitere Quellen des Artikels sind unter ix.de/zstk zu finden).

In Ergänzung zu den bekannten Standards von NIST und ISO/IEC existieren diverse weitere Veröffentlichungen, die wertvolle Unterstützung im Bereich der Reaktionsplanung bieten. Im deutschsprachigen Raum zählen dazu insbesondere die Publikationen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Ebenso sind der „Leitfaden für bewährte Praktiken zum Management von Vorfällen“ der ENISA (Agentur der Europäischen Union für Cybersicherheit) sowie das „Computer Security Incident Response Team Service Framework“ von FIRST (Forum der Vorfallreaktions- und Sicherheitsteams) zu nennen (siehe ix.de/zstk). Diese beiden Veröffentlichungen richten sich jedoch vorrangig an größere Organisationen.

iX-TRACT

- Durch eine sorgfältige Vorbereitung sind Beteiligte in der Lage, angemessen auf Sicherheitsvorfälle zu reagieren. Das ermöglicht es, Sicherheitsvorfälle von Anfang an einzudämmen und somit negative Auswirkungen und Kosten zu minimieren.
- Internationale Standards im Bereich der Notfallvorsorge stellen eine wertvolle Ressource für die Vorbereitung auf Sicherheitsvorfälle dar. Sie können dabei unterstützen, sich umfänglich vorzubereiten oder bereits eingeführte Verfahren zu überprüfen und zu optimieren.
- Alle relevanten Standards empfehlen einen ganzheitlichen Ansatz, der sämtliche Phasen eines Sicherheitsvorfalls berücksichtigt – er reicht von der Vorbereitung bis hin zur kontinuierlichen Überprüfung und gegebenenfalls Verbesserung des Reaktionsplans.

Welcher Standard für wen?

Die Auswahl des Standards für die Reaktionsplanung ist zweifellos von großer Bedeutung. Noch entscheidender ist jedoch, dass überhaupt ein Standard verwendet wird. Sofern das Ziel eines Unternehmens nicht darin besteht, die Reaktion als externe Dienstleistung anzubieten oder für ein äußerst komplexes Unternehmen aufzubauen, werden in der Regel die NIST- oder ISO/IEC-Standards ausreichen. Der NIST-Standard bietet den Vorteil, dass er kostenlos verfügbar und nicht urheberrechtlich geschützt ist, was bedeutet, dass er frei genutzt werden kann.

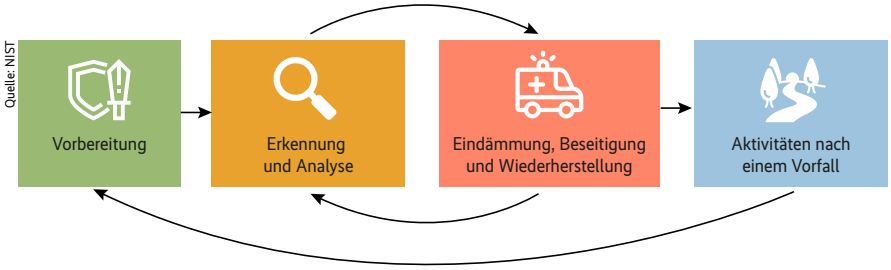
Im Gegensatz dazu kostet ein Teil der ISO/IEC-27035-Reihe etwa 150 bis 200 Euro. Insbesondere empfiehlt sich die Nutzung dieses Standards, wenn ein Unternehmen eine ISO/IEC-27001-Zertifizierung anstrebt oder diese bereits vorhanden ist und die entsprechenden Maßnahmen zur Reaktionsplanung implementiert werden sollen. Ein weiterer Grund für den Einsatz dieses Standards könnte eine enge Zusammenarbeit bei der Bewältigung von Sicherheitsvorfällen mit bereits zertifizierten Partnerunternehmen sein, da sich dadurch der Reaktionsplan leichter angleichen lässt.

Da für die meisten Unternehmen der NIST- oder ISO/IEC-Standard ausreichend sein sollte und sie weltweit etabliert sind, wird sich dieser Artikel primär auf diese beiden konzentrieren.

Die Abläufe im Vergleich

Alle Standards und Empfehlungen stimmen darin überein, dass eine ganzheitliche Betrachtung von der Planung bis hin zur kontinuierlichen Verbesserung von großer Bedeutung ist. Der vom NIST und der von der ISO/IEC definierte Prozess für die Reaktion auf Sicherheitsvorfälle ähneln einander in vielen Aspekten. Vergleichbare Prozessabläufe lassen sich meist in anderen Standards und Empfehlungen finden, was darauf hindeutet, dass sie möglicherweise auf NIST und/oder ISO/IEC aufbauen. NIST definiert in seinem Prozess vier Phasen und betont dabei, dass diese nicht sequenziell sind, sondern einen Kreislauf bilden (siehe Abbildung 1).

In der ersten Phase, der Vorbereitung, geht es um den Aufbau der Notfallorganisation und das Training sowie um die Beschaffung der erforderlichen Tools und Ressourcen. Zudem zielt diese Phase darauf ab, die Anzahl von Sicherheitsvorfällen durch präventive Maßnahmen zu reduzieren. Die nächste Phase, „Erkennung und Analyse“, konzentriert sich auf die Erkennung von Sicherheitsvorfällen durch die Analyse der Sicherheitsmeldungen von Systemen und Mitarbeitenden. Die Phase umfasst auch die Priorisierung anhand bestimmter Kriterien, falls mehrere Sicherheitsvorfälle gleichzeitig auftreten, sowie die Benachrichtigung relevanter Stakeholder wie des höheren Managements und der Mitglieder der Notfallorganisation.



So sieht der Prozess zur Bewältigung eines Sicherheitsvorfalls nach NIST SP 800-61 Revision 2 aus (Abb. 1).

Die dritte Phase, „Eindämmung, Beseitigung und Wiederherstellung“, beschreibt die Reaktion auf einen erkannten Sicherheitsvorfall. Das Ziel dieser Phase besteht darin, den Vorfall einzudämmen und alle betroffenen Systeme in ihren Normalzustand zurückzuführen. NIST betont an dieser Stelle, dass oft zur Analyse der vorherigen Phase zurückgekehrt werden muss, um beispielsweise zusätzlich betroffene Systeme zu identifizieren. Sobald der Sicherheitsvorfall erfolgreich behandelt wurde, beginnt die vierte und letzte Phase, „Aktivitäten nach einem Vorfall“. In dieser Phase werden die Erkenntnisse aus der Vorfallbewältigung genutzt, um sowohl die Reaktionsplanung als auch die Sicherheitsmaßnahmen zu verbessern. Mit dieser Verbesserung schließt sich der Kreislauf und kehrt zur ersten Phase des Prozesses zurück.

Nur Detailunterschiede

ISO/IEC 27035 unterscheidet zwischen fünf Phasen (siehe Abbildung 2), eine mehr als NIST. Die erste Phase, „planen und vorbereiten“, und die letzte, „lernen“, entsprechen der ersten und letzten Phase von NIST. Die vierte Phase bei ISO/IEC, „reagieren“, entspricht bei NIST „Eindämmung, Beseitigung und Wiederherstellung“. Der Hauptunterschied zu NIST besteht darin, dass die NIST-Phase „Erkennung und Analyse“ in den zwei Phasen „erkennen und melden“ und „bewerten und entscheiden“ abgebildet wird. Trotz dieser Unterschiede bleibt der inhaltliche Kern beider Standards nahezu identisch. Wie bei NIST wird auch bei ISO/IEC der Prozess als Kreislauf dargestellt, wobei Erkenntnisse aus Sicherheitsvorfällen kontinuierlich zur Verbesserung beitragen.

Zusätzlich zu den fünf Prozessphasen listet ISO/IEC 27035 Tätigkeiten auf, die in allen Phasen erfolgen. Diese sind bei NIST lediglich implizit enthalten. Eine der wichtigsten Tätigkeiten ist die fortlaufende Dokumentation des Sicherheitsvorfalls und der getroffenen Maßnahmen. Ebenfalls hebt ISO/IEC 27035 die fortlaufende Koordination beziehungsweise Kommunikation zwischen interessierten Parteien hervor. Zu diesen Parteien zählt der Standard unter anderem die Mitglieder der Notfallorganisation, das Management, Mitarbeitende und Partnerfirmen.

Beide Standards betonen die Wichtigkeit einer gründlichen Vorbereitung. Wie schon beschrieben zählt hierzu auch die Prävention, die gewährleisten soll, dass Systeme, Netzwerke und Anwendungen ausreichend gesichert sind. Die Standards empfehlen einen ganzheitlichen Ansatz, der sämtliche Phasen eines Sicherheitsvorfalls berücksichtigt. Dazu gehören unter anderem die Ausarbeitung der Rahmenbedingungen, der zu erbringenden Dienstleistungen, der Struktur der Notfallorganisation, der zu besetzenden Rollen, des Reaktionsplans inklusive Standardarbeitsanweisungen (Standard Operating Procedures; SOPs), der Protokollvorlage, des Kommunikationsplans und das Durchführen von regelmäßigen Übungen. Im Nachfolgenden werden diese Punkte ausführlicher beschrieben.

Rahmenbedingungen klären und festhalten

Die Grundlage für sämtliche Schritte und Überlegungen im Umgang mit Sicherheitsvorfällen sind die definierten Rahmenbedingungen. Daher ist es entscheidend, dass sie geklärt und schriftlich festgehalten werden. Wie bei allen Projekten ist es von großer Bedeutung, dass das höhere Management seine Unterstützung zusichert, um sicherzustellen, dass die

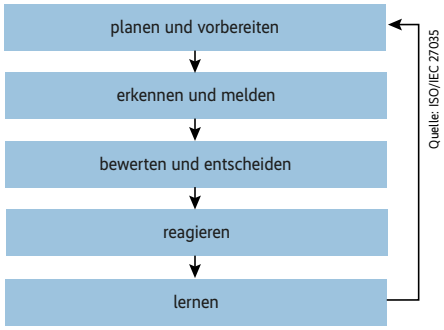
erforderlichen Ressourcen bereitgestellt werden. Ein weiterer wichtiger Aspekt ist die Festlegung des Zuständigkeitsbereichs, der die Zusammensetzung der Notfallorganisation sowie die angebotenen Dienstleistungen beeinflusst. Die Verantwortlichen müssen zunächst definieren, für welche Arten von Vorfällen die Notfallorganisation zuständig ist. Hierbei ist zu klären, ob dies nur Sicherheitsvorfälle im Zusammenhang mit der IT-Infrastruktur betrifft oder beispielsweise auch physische Ereignisse wie den Verlust sensibler Geschäftsunterlagen. Diese Entscheidung hängt in der Regel von der Unternehmensstruktur und -größe ab.

Des Weiteren ist festzulegen, welche Vorfälle die jeweiligen Fachbereiche eigenständig bewältigen können, ab welchem Zeitpunkt die Notfallorganisation eingreifen sollte und wann eine Eskalation an den Krisenstab erforderlich ist. Eine mögliche Vorgehensweise könnte folgendermaßen aussehen: Der Fachbereich behebt kleinere Sicherheitsvorfälle ohne wesentliche Auswirkungen auf das Unternehmen und/oder den Betrieb eigenständig (zum Beispiel simples Phishing). Die Notfallorganisation schreitet ein, sobald der Geschäftsbetrieb voraussichtlich beeinträchtigt sein wird oder ein Schutzziel der Informationssicherheit, wie Vertraulichkeit, Integrität und Verfügbarkeit, gefährdet ist (etwa Befall eines Systems durch Schadsoftware). Die Eskalation an den Krisenstab erfolgt bei Situationen, die außer Kontrolle geraten sind, sodass der Normalbetrieb sich in absehbarer Zeit nicht wiederherstellen lässt (beispielsweise Angriff durch Ransomware).

Idealerweise werden für diese Entscheidungen objektive Kriterien festgelegt, wie die Kritikalität der betroffenen Systeme oder die Anzahl der betroffenen Mitarbeitenden und Kunden. Ein weiterer wesentlicher Aspekt betrifft die Festlegung von Notfallrechten. Diese können beispielsweise die Befugnisse enthalten, in einem Sicherheitsvorfall Sofortmaßnahmen zu ergreifen oder ein fortlaufendes Sicherheitsmonitoring einzurichten, das gegebenenfalls auch vertrauliche Informationen umfasst. Es ist ratsam, die festgelegten Befugnisse, die alle Mitarbeitenden betreffen, transparent zu kommunizieren. Das Mitarbeiterhandbuch kann beispielsweise als zentrale Informationsquelle dienen.

Dienstleistungsportfolio aufstellen

Basierend auf den Rahmenbedingungen setzen sich die Dienstleistungen der Notfallorganisation zusammen. Neben den Tätigkeiten, die direkt mit der Reaktion auf einen Sicherheitsvorfall zusammenhängen, sollte man im Sinne der ganzheitlichen Betrachtung definieren, welche weiteren Tätigkeiten die Notfallorganisation übernehmen und bei welchen sie unterstützen kann.



Trotz feiner Unterschiede ist das Prinzip des Vorfallsbehandlungsmodells nach ISO/IEC 27035 dasselbe wie beim NIST-Standard (Abb. 2).

Ein wichtiger Aspekt ist das Erkennen potenzieller Sicherheitsvorfälle. Zum einen sollte man ein technisches Sicherheitsmonitoring in Betracht ziehen, mit dem Abweichungen vom Normalbetrieb zeitnah erkannt und untersucht werden können. Hier ist einzuplanen, zu welchen Zeiten (rund um die Uhr oder nur zu Arbeitszeiten?), innerhalb welcher Frist (zum Beispiel kritische Meldungen innerhalb von 30 Minuten) und von wem (dedizierter Analyst oder IT-Team?) diese gemeldeten Abweichungen untersucht werden.

Zum anderen gilt es zu klären, wie und an wen Mitarbeitende und externe Parteien Auffälligkeiten melden können. Die Standards empfehlen, eine zentrale Anlaufstelle einzurichten, die solche Meldungen entgegennehmen kann. Zudem wird die Schaffung einer Unternehmenskultur empfohlen, in der Sicherheitsvorfälle ohne Furcht vor negativen Konsequenzen gemeldet werden können. Mitarbeitende sollten ermutigt werden, Vorkommnisse offen und ehrlich zu melden, ohne befürchten zu müssen, dass dies Nachteile für sie haben könnte. Auf diese Weise lässt sich vermeiden, dass Sicherheitsvorfälle aus Angst vor Konsequenzen verschwiegen werden.

Alternativ empfiehlt es sich, einen anonymen Meldeweg einzurichten. Außer dem Erkennen und Bewältigen von Sicherheitsvorfällen kann die Notfallorganisation auch weitere Tätigkeiten erbringen oder bei diesen unterstützen. Dazu gehört das Schwachstellenmanagement, das die Erkennung, Analyse und Koordination der Behebung von Schwachstellen umfasst. Des Weiteren kann die Notfallorganisation bei der Bewertung von Risiken und Bedrohungen unterstützen sowie über neue Bedrohungen und Erkenntnisse aus Sicherheitsvorfällen informieren – auch außerhalb des Unternehmens. Diese Informationen lassen sich auch für Awareness- und Trainingskampagnen nutzen.

Notfallorganisation strukturieren

Sind die Rahmenbedingungen und die zu erbringenden Dienstleistungen festgelegt, kann die Struktur der Notfallorganisation definiert werden. Eine typische Überlegung ist, ob es nur eine zentrale Notfallorganisation oder mehrere verteilte Teams geben soll. Kleinere Firmen oder Firmen, deren IT-Ressourcen zentral verwaltet werden, entscheiden sich in der Regel für die erste Variante. Die zweite Option ist oft in großen, weltweit verteilten Firmen zu finden. Diese Firmen können beispielsweise für jede Region oder jeden größeren Standort ein eigenes Notfallteam aufbauen, wobei die zentrale Koordination nicht vergessen werden darf.

Eine weitere typische Überlegung ist, ob alle Tätigkeiten innerhalb der Firma durchgeführt werden oder ob eine Teilauslagerung an einen externen Dienstleister sinnvoll ist. In der Praxis wird das Sicherheitsmonitoring, also die technische Überwachung auf Abweichungen vom Normalbetrieb, oft ausgelagert, da hierdurch eine durchgehende Überwachung erschwinglich wird. Ebenso werden spezifische Reaktionstätigkeiten, beispielsweise die tiefgehende technische Analyse von Schadsoftware, ausgelagert, damit das Fachwissen nicht innerhalb der Firma aufgebaut werden muss.

Typische Rollen in der Notfallorganisation

Sobald die Struktur festgelegt ist, können die erforderlichen Rollen eingeteilt werden. In der Regel wird es eine leitende Person mit Stellvertretung geben. Diese Person trägt die fachliche Verantwortung für die Reaktionsplanung sowie die Notfallorganisation und entwickelt diese zwei Bereiche stetig weiter. Bei einem Sicherheitsvorfall übernimmt sie die Kommunikation mit dem höheren Management und anderen Anspruchsgruppen sowie die Koordination der involvierten Personen. Je nach Firmengröße kann es neben der fachlichen Leitung auch eine technische Leitung ge-

ben, die für die technische Qualität der Ergebnisse der Notfallorganisation zuständig ist und daher IT-Sachkenntnis in diversen Bereichen mitbringen sollte. Ebenfalls kann es in größeren Unternehmen eine leitende Person pro Sicherheitsvorfall geben, sollten mehrere Vorfälle parallel auftreten.

In kleineren Unternehmen kann es dagegen sein, dass diese drei Rollen von einer einzigen Person ausgeübt werden. Der Hauptbestandteil der Notfallorganisation setzt sich in der Regel aus technischen Experten zusammen, die auftretende Ereignisse analysieren und im Falle eines Sicherheitsvorfalls die Bewältigung übernehmen. Diese Mitglieder der Notfallorganisation sollten eine breite Palette an technischen Fähigkeiten abdecken, darunter Systemadministration, Netzwerkadministration, Programmierung und technischer Support. Idealerweise sollte für jedes häufig angegriffene Betriebssystem und jede Anwendung mindestens ein Experte vorhanden sein.

Neben diesen zentralen Rollen gilt es weitere zu berücksichtigen, die entweder Teil der Notfallorganisation sind oder mit denen ein enger Kontakt gepflegt werden sollte. Allen voran stehen externe Dienstleister, beispielsweise IT-Dienstleister, die in kritischen Fällen zur Reaktion hinzugezogen werden müssen. Je nach Fall muss auch die Kommunikationsabteilung einbezogen werden, um die interne und externe Kommunikation zu koordinieren. Auch sollten Mitarbeitende aus dem Personalwesen frühzeitig kontaktiert werden, falls absehbar ist, dass Überstunden und/oder Wochenendarbeit erforderlich sein werden.

Weitere Rollen können beispielsweise die Datenschutzbeauftragten, die Rechtsabteilung oder die physische Sicherheit sein. Eine beispielhafte Notfallorganisation ist in Abbildung 3 abgebildet. Abschließend ist festzulegen, wann und in welchem Umfang die Mitglieder der Notfallorganisation in ihrer Funktion tätig sind. Häufig nehmen die meisten Mitglieder nur vorübergehend während eines Sicherheitsvorfalls diese Rollen ein und bekleiden sonst eine andere Position im Unternehmen.

Reaktionsplan und Standardarbeitsanweisungen ausarbeiten

Der Reaktionsplan enthält alle wichtigen Informationen für das Vorgehen in einem Sicherheitsvorfall. Er sollte einen einfachen und leicht verständlichen Prozess enthalten, der geübt und getestet wurde. Unter ix.de/zstk findet sich ein beispielhaftes und vereinfachtes Flussdiagram, das die Bewältigung eines Sicherheitsvorfalls nach ISO/IEC 27035 verdeutlicht.

Idealerweise orientiert sich der Prozess an einem der Standards, um sicherzustellen, dass alle erforderlichen Schritte berücksichtigt werden. Es ist von besonderer Bedeutung, klare Verantwortlichkeiten festzulegen, damit eindeutig ist, wer für welche Aufgaben verantwortlich ist und welcher Zeitrahmen für deren Erledigung gilt. Fehlt diese Festlegung, besteht die Gefahr, dass Tätigkeiten nicht oder nur zeitverzögert durchgeführt werden, wodurch wertvolle Zeit bei der Bewältigung von Sicherheitsvorfällen verloren geht.

Eine weitere Quelle für Verzögerungen ist die verspätete Entscheidung, ob die Notfallorganisation zusammentreten oder sogar der Krisenstab aktiviert werden muss. In der Praxis haben Unternehmen oft Schwierigkeiten, diese Entscheidung zu treffen, weshalb der Reaktionsplan an dieser Stelle objektive Vorgaben machen sollte. Ebenfalls sollte der Reaktionsplan definieren, wie die Übergabe an diesen Stellen funktioniert und wer informiert werden muss.

Sind Partnerfirmen, beispielsweise IT-Provider, in den Reaktionsplan involviert, muss deren Rolle bekannt sein. Weiterhin sollte der Reaktionsplan so abgelegt werden, dass er selbst bei einem Ausfall der zentralen IT-Systeme zugänglich ist. Dies kann beispielsweise durch das Speichern außerhalb des zentralen Netzwerks oder durch das Aufbewahren in Papierform geschehen. Wird der Plan ausgedruckt, sind bei einer Aktualisierung alle alten Exemplare auszutauschen.

Typische Angriffsszenarien ermitteln

Neben dem Reaktionsplan empfiehlt es sich, Standardarbeitsanweisungen (SOPs) für typische Angriffsvektoren zu erstellen. Die SOPs legen detailliert fest, wie beim Eintreten eines spezifischen Sicherheitsvorfalls vorzugehen ist, um die Qualität und Schnelligkeit der Reaktion sicherzustellen und somit den Schaden zu minimieren. Die Standards listen gängige Angriffsvektoren auf, die als Grundlage für die Entwicklung entsprechender SOPs dienen können. Beispiele hierfür sind E-Mail-Angriffe wie Phishing, externe Speichermedien wie USB-Sticks, Brute-Force- und weitere webbasierte Angriffe sowie der Diebstahl oder Verlust von Geräten. Durch eine gezielte Analyse der häufig auftretenden Angriffsvektoren können Unternehmen bestimmen, welche SOPs entwickelt werden sollten, um angemessen auf gängige Bedrohungen zu reagieren.

Bei der Ausarbeitung eines Reaktionsplans und der SOPs gilt es zu berücksichtigen, dass Prozesse und Checklisten oft eine schrittweise Abfolge der Reaktion vorschlagen. Jedoch müssen während eines Sicherheitsvorfalls, wie bereits in einem Artikel zu Playbooks für Sicherheitsvorfälle [1] gezeigt, Aktivitäten auch parallel durchgeführt werden oder es kann sogar notwendig sein, einen Schritt zurückzugehen. Daher sollten die Pläne nicht zu starr formuliert sein.

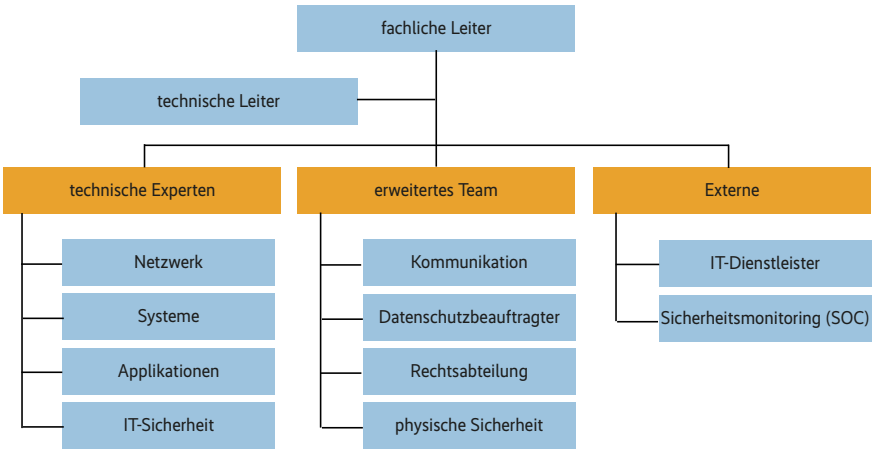
Protokoll vorbereiten

Bei einem Sicherheitsvorfall ist es gemäß den Standards von entscheidender Bedeutung, alle relevanten Informationen festzuhalten. Dies hilft den beteiligten Personen, den aktuellen Stand und die getroffenen Maßnahmen nachzuvollziehen, und ist besonders dann relevant, wenn sich der Sicherheitsvorfall in die Länge zieht oder mehrere Mitarbeitende und Parteien involviert sind. Eine lückenlose Dokumentation ist auch hilfreich für die spätere Aufbereitung des Sicherheitsvorfalls sowie für die Ableitung von Verbesserungen in der Reaktionsplanung und den Sicherheitsmaßnahmen.

Die Notfallorganisation sollte alle relevanten Informationen zu einem Sicherheitsvorfall umgehend dokumentieren. Dazu gehören der aktuelle Status des Vorfalls, eine Zusammenfassung der Ereignisse, erste Anzeichen, eine Einschätzung der Auswirkungen, eine Liste des gesammelten Beweismaterials, die beteiligten Personen sowie eine chronologische Aufzeichnung von Maßnahmen und Entscheidungen mit verantwortlichen Personen. Um sicherzustellen, dass nichts vergessen oder unvollständig erfasst wird, ist es ratsam, im Vorfeld eine Protokollvorlage zu erstellen.

Kommunikation zentral steuern

Empfehlungen von Standards sehen das Erstellen eines Kommunikationsplans als integralen Bestandteil der Vorbereitung auf Sicherheitsvorfälle vor, in der Praxis wird dieser jedoch häufig vernachlässigt. [2] zeigt, dass ein solcher Plan hilft, im Falle eines Sicherheitsvorfalls schnell und effektiv zu kommunizieren. Das ist entscheidend, um Informationen über den Vorfall zu steuern – vom Zeit-



So kann beispielsweise eine auf ISO/IEC und NIST basierende, an das Unternehmen angepasste Notfallorganisation aussehen (Abb. 3).

punkt und Inhalt bis hin zur Art und Weise, wie sie übermittelt werden. Auf diese Weise können Gerüchte vermieden und die Wahrnehmung von Einzelpersonen und der Öffentlichkeit kann beeinflusst werden. Sobald mit Externen wie Kunden oder Partnerfirmen kommuniziert werden soll, ist es ratsam, dass die gesamte Kommunikation über einen zentralen Ansprechpartner oder eine zentrale Anlaufstelle läuft, die im Umgang mit Medien geschult ist. Die zentrale Anlaufstelle muss über die aktuellen Geschehnisse des Sicherheitsvorfalls informiert bleiben, damit die Kommunikation stets aktuell und konsistent ist.

Bei der Kommunikation ist entscheidend, dass keine vertraulichen Informationen preisgegeben werden, beispielsweise technische Details der getroffenen Sofortmaßnahmen, da das zusätzliche Ansatzpunkte für Angreifer bieten kann. Alle Mitarbeitenden müssen zudem im Vorfeld geschult werden, mögliche Presseanfragen auf die zentrale Anlaufstelle zu verweisen und Informationen nicht auf eigene Faust an Dritte weiterzugeben. Denn nichts ist schädlicher als Gerüchte, Halbwahrheiten oder Insiderwissen, die über unautorisierte Kanäle verbreitet werden und die offizielle Kommunikation torpedieren. Ein weiterer Aspekt eines Kommunikationsplans betrifft die Kommunikation mit externen Partnern wie IT-Dienstleister oder externe Mitarbeitende. Mit diesen sollte man im Vorfeld eine Geheimhaltungsvereinbarung treffen, damit im Falle eines Sicherheitsvorfalls Informationen ausgetauscht werden können.

Ergänzend zur externen Kommunikation kann auch die interne Kommunikation vorbereitet werden. Hier kann man zwischen der Kommunikation innerhalb der Notfallorganisation, mit allen Mitarbeitenden sowie internen Anspruchsgruppen wie dem höheren Management oder Systemverantwortlichen unterscheiden. Bei allen drei Gruppen empfiehlt es sich, im Voraus festzulegen, wer welche Informationen über welchen Kanal und zu welchem Zeitpunkt teilt. Dabei gilt es zu bedenken, dass Kommunikationsmittel wie E-Mail oder Videokonferenztools bei einem Sicherheitsvorfall ausfallen oder kompromittiert sein können, weshalb alternative Kontaktmöglichkeiten vorhanden sein sollten. Hierfür bietet sich die Erstellung einer Kontaktliste an, die je Primär- und Sekundärkontakt neben der geschäftlichen Telefonnummer und E-Mail-Adresse auch alternative Kontaktmöglichkeiten enthält, etwa private Telefonnummern. Auch ist zu überlegen, ob zusätzliche Notfalltools für die Kommunikation vorbereitet werden sollten.

Insgesamt ist ein gut durchdachter Kommunikationsplan von entscheidender Bedeutung, um im Falle eines Sicherheitsvorfalls angemessen und effektiv reagieren zu können. Er ermöglicht eine koordinierte und zielgerichtete Kommunikation, sowohl intern als auch extern, und trägt somit maßgeblich zur erfolgreichen Bewältigung von Sicherheitsvorfällen bei.

Ein Plan kann noch so gut sein …

Ist der Reaktionsplan erstellt, muss sichergestellt sein, dass er der Realität entspricht und alle Beteiligten ihre Rollen und Aufgaben kennen. Dazu empfehlen sich Notfallübungen. In der Praxis hat sich vor allem gezeigt, dass die Beteiligten gerade am Anfang eher zögerlich reagieren, vor allem wenn produktive Systeme abzustellen sind oder an das höhere Management eskaliert werden muss. Die Standards empfehlen, zunächst zu bestimmen, warum eine Übung durchgeführt werden soll, damit auf dieser Grundlage geplant werden kann. Je nachdem, ob ein neuer Reaktionsplan validiert, Mitarbeitende trainiert oder ein bestehender Plan auf seine Gültigkeit überprüft werden sollen, kann die Übung als Diskussion, als Szenario in Form einer Tabletop- oder als Liveübung durchgeführt werden.

Welche Form auch immer gewählt wird, es muss entschieden werden, wer alles hinzugezogen werden soll – ob beispielsweise auch externe Partner, die bei Sicherheitsvorfällen involviert sein können, in die Übung einbezogen werden sollen. Für Inspiration zur Erstellung einer Übung lässt sich der Anhang von NIST zurate ziehen, der verschiedene Szenarien mit Fragen enthält.

Fazit

Um Sicherheitsvorfälle zeitnah zu bewältigen und die entstehenden Kosten niedrig zu halten, ist eine gründliche und umfassende Vorbereitung nötig. Standards wie die von NIST und ISO/IEC können dabei helfen, alle nötigen Schritte zu bedenken, und geben praktische Hinweise zur Umsetzung. Zu den Schritten gehören die Ausarbeitung der Rahmenbedingungen, der zu erbringenden Dienstleistungen, der Struktur der Notfallorganisation, der zu besetzenden Rollen, des Reaktionsplans inklusive Standardarbeitsanweisungen (SOPs), der Protokollvorlage, des Kommunikationsplans und das Durchführen von regelmäßigen Übungen. (ur@ix.de)

Quellen

[1] Jerome Horn, Dominik Seidel; Mit Playbooks auf Sicherheitsvorfälle reagieren; iX 5/2023, S. 90
[2] Marcel Herder, Jan Frongia; ITSCM: Vorbereitet für den Cyber-Ernstfall; iX 5/2024, S. 86
[3] Die zitierten Standards und Guidelines sind über ix.de/zstk zu finden.

JAN HUCK

ist Senior Cyber Response and Security Consultant bei der Oneconsult AG. Er bietet weitreichende CISO-Services an, darunter im Bereich Vorbereitung auf Sicherheitsvorfälle.