Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Incident Response

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

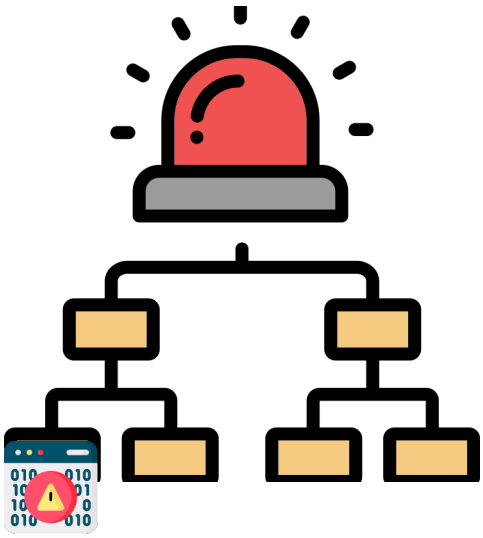
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Incident Response – Was ist das?

Incident Response bezeichnet die **systematische Vorgehensweise**, mit der Organisationen auf Sicherheitsvorfälle im Zusammenhang mit Informationssystemen und Netzwerken reagieren. Dabei geht darum, einen **Vorfall zu identifizieren und einzudämmen** sowie dessen Ursachen zu analysieren, um zukünftige Vorfälle zu verhindern oder deren Auswirkungen zu minimieren. Ein effektiver Incident Response-Prozess umfasst typischerweise die Schritte Vorbereitung, Erkennung, Eindämmung, Beseitigung, Wiederherstellung und Nachbereitung.



Welche Maßnahmen sind erforderlich?

Die Einführung von Incident Response in einem Unternehmen oder einer Institution erfordert zunächst eine **Bestandsaufnahme** der vorhandenen Sicherheitsinfrastruktur und -prozesse. Hierzu zählt beispielsweise die Identifikation kritischer Systeme und Daten, die Bewertung der aktuellen Schutzmaßnahmen sowie die Analyse von potenziellen Schwachstellen und die Konsequenzen einer Störung.

Im nächsten Schritt muss definiert werden, wie Störungen im Betrieb, Notfälle und Krisen bzw. Katastrophen unterschieden werden können, um **Reaktionsmuster** daraufhin abstimmen zu können. Des Weiteren sollte ein **Incident Response-Team** gebildet werden, das aus Fachleuten mit unterschiedlichen Kompetenzen besteht, wie zum Beispiel IT-Sicherheit, Netzwerktechnik, Datenschutz und Kommunikation. Dieses Team ist für die Planung, Durchführung und Kontrolle der Maßnahmen verantwortlich.

Die **Entwicklung eines Incident Response-Plans** ist ebenfalls ein wichtiger Bestandteil des Incident Response-Managements. Dieser Plan legt fest, wie im Falle eines Sicherheitsvorfalls vorgegangen wird und welche Ressourcen dafür zur Verfügung stehen. Er sollte **regelmäßig überprüft und aktualisiert** werden, um sich an die sich ständig ändernden Bedrohungen und Technologien anzupassen.

Cyber-Sicherheitsrat Deutschland e.V.

Arten von Incident Response-Maßnahmen

Incident Response zeigt sich in unterschiedlichen Facetten, abhängig von der Art des Sicherheitsvorfalls und den speziellen Anforderungen der betroffenen Organisation. Beispielsweise fokussiert die **proaktive Incident Response** vorbeugende Maßnahmen wie Penetrationstests, Sicherheitsaudits und kontinuierliches Monitoring der IT-Systeme, um potenzielle Sicherheitsvorfälle frühzeitig aufzuspüren und abzuwenden. Im Gegensatz dazu liegt der Schwerpunkt der **reaktiven Incident Response** auf der Bewältigung bereits eingetretener Sicherheitsvorfälle, um den entstandenen Schaden einzudämmen und die Ursachen zu analysieren, mit dem Ziel, zukünftige Vorfälle zu verhindern.

Zudem kann es vorkommen, dass Organisationen externe Experten heranziehen, um bei der Untersuchung und Behebung von Sicherheitsvorfällen zu unterstützen. Dieser Ansatz (**externe Incident Response**) kommt insbesondere dann zum Tragen, wenn das interne Incident Response-Team nicht über genügend Ressourcen oder Erfahrungen verfügt, um einen Vorfall effizient zu bewältigen. Insgesamt bieten die verschiedenen Formen Organisationen vielfältige Möglichkeiten, ihre Cybersicherheit den individuellen Gegebenheiten und Anforderungen entsprechend zu gestalten und zu stärken.

Zur Planung der Reaktion auf einen Sicherheitsvorfall muss ebenso bedacht werden, wie der **Geschäftsbetrieb während der Notfallsituation** aufrechterhalten werden kann. Hierzu sind Risiken und Maßnahmen zu bestimmen und entsprechende Vorbereitungen zu veranlassen, die wie ein Drehbuch ausgeführt werden können. So ein Drehbuch erarbeitet man idealerweise in konkreten **Notfallsimulationen**. Incident Response kann auch durch technische Geräte, wie moderne Firewalls, **(teil-)automatisiert** gelöst werden.

Wem nutzt Incident Response?

Der Adressatenkreis umfasst eine breite Palette von Organisationen, darunter Unternehmen, Regierungsbehörden, gemeinnützige Organisationen und Bildungseinrichtungen. Grundsätzlich sollte jedes Unternehmen oder jede Institution, das bzw. die mit sensiblen Daten arbeitet oder von Cyberbedrohungen betroffen sein könnte, Incident Response in Erwägung ziehen.

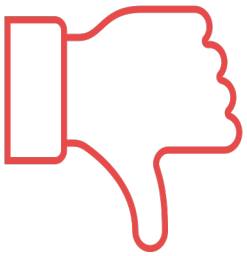
Die Größe und Art der Organisation spielt dabei eine Rolle bei der Gestaltung des Prozesses, aber **grundlegende Prinzipien und Best Practices gelten für alle Organisationen**, unabhängig von ihrer Größe und Branche.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Chancen gibt es?

Eine **verbesserte Sicherheitslage** ergibt sich durch einen strukturierten Incident Response-Prozess, der Sicherheitsvorfälle schneller und effektiver erkennt und behebt. Dies trägt zur allgemeinen Stärkung der Sicherheit der Organisation bei und unterstützt zudem die **Einhaltung von Compliance- und regulatorischen Anforderungen**, die in vielen Branchen und Ländern bezüglich Cybersicherheit und Datenschutz gelten. Dadurch können mögliche **Sanktionen vermieden** werden.
Ein weiterer Vorteil eines effektiven Incident Response-Managements ist der Schutz des Unternehmensrufs. Indem das Vertrauen von Kunden, Partnern und anderen Stakeholdern erhalten bleibt, wird die **Reputation der Organisation** gewahrt. Insgesamt zeigt sich, dass die Implementierung von Incident Response eine wichtige Rolle dabei spielt, die Sicherheit und Stabilität von Unternehmen und Institutionen in der digitalen Welt zu gewährleisten.

Welche Risiken gibt es?



Die Einführung und Aufrechterhaltung eines effektiven Prozesses erfordert sowohl **finanzielle als auch personelle Ressourcen**. Dies kann für Unternehmen und Institutionen eine erhebliche Belastung darstellen. Ein weiteres Risiko, das bei der Implementierung von Incident Response-Maßnahmen auftreten kann, sind **Fehlalarme**. Dies kann unnötige Ressourcenverwendung und möglicherweise negative Auswirkungen auf das Geschäft zur Folge haben. Es ist daher wichtig sicherzustellen, dass die Incident Response-Maßnahmen **angemessen auf die Bedrohungslandschaft abgestimmt** sind, um Fehlalarme zu minimieren.
Schließlich kann die **fehlende Einbindung des Managements** den Erfolg der Incident Response beeinträchtigen. Wenn das Management eines Unternehmens oder einer Institution die Bedeutung nicht erkennt und entsprechende Ressourcen nicht bereitstellt, kann dies den Erfolg der Maßnahmen beeinträchtigen. Insgesamt gilt es, die Risiken und Nachteile im Rahmen der jeweiligen Organisationsstruktur sorgfältig abzuwägen und angemessen zu berücksichtigen.

Fazit

Incident Response ist eine **wesentliche Komponente der Cybersicherheitsstrategie** von Unternehmen und Institutionen in der heutigen vernetzten Welt. Durch die Implementierung von Incident Response-Maßnahmen können Organisationen ihre **Sicherheitslage verbessern**, Schäden durch Cyberangriffe minimieren und das Vertrauen von Kunden, Partnern und anderen Stakeholdern bewahren.
Die Einführung von Incident Response erfordert jedoch eine s**orgfältige Planung, ausreichende Ressourcen und die Einbindung aller Mitarbeiter** und Führungskräfte. Organisationen sollten daher den Prozess der Implementierung von Incident Response nicht unterschätzen und bereit sein, in die nötigen Ressourcen zu investieren, um ihre Cybersicherheit langfristig zu gewährleisten und ihre Organisation vor Cyberbedrohungen zu schützen.

Cyber-Sicherheitsrat Deutschland e.V.