Erstellung eines Incident-Management- & Response-Konzepts für die CURSOR Software AG

Maximilian Marx

Technische Hochschule Mittelhessen

Fachbereich MND
Wilhelm-Leuschner-Str. 13
61169 Friedberg
E-Mail:
maximilian.marx@mnd.thm.de

Prof. Dr. Harald Ritz

Technische Hochschule Mittelhessen

Fachbereich MNI
Wiesenstraße 14
35390 Gießen
E-Mail:
harald.ritz@mni.thm.de

Prof. Dr. Frank Kammer

Technische Hochschule Mittelhessen

Fachbereich MNI
Wiesenstraße 14
35390 Gießen
E-Mail:
frank.kammer@mni.thm.de

Kategorie

Masterarbeit

Schlüsselwörter

IT-Security, Incident Response Management, Security Incidents, Hacking, Cybersecurity

Zusammenfassung

Die vorliegende Masterarbeit umfasst die Erstellung eines Incident-Management- & Response-Konzepts angepasst an die internen Strukturen und Anforderungen der CURSOR Software AG.

Die CURSOR Software AG ist ein Hersteller von CRM-Systemen mit Hauptsitz in Gießen. Das CRM-System wird überwiegend bei Energiedienstleistern eingesetzt. Innerhalb von CRM-Systemen werden zum Großteil personenbezogene Daten gespeichert. Hierbei handelt es sich um Informationen, worüber einzelne Personen eindeutig identifiziert werden können. Diese Art von Daten unterliegen nach deutschem und europäischem Datenschutzrecht besonderen Vorschriften und Sicherungsvorkehrungen.

Cyberangriffe auf Unternehmen sind mittlerweile zu etwas alltäglichen geworden. Dabei stellt der Einsatz von Sicherheitssystemen keinen ausreichenden Schutz mehr dar, sondern es Bedarf sowohl personeller als auch organisatorischer Maßnahmen, um Sicherheitsvorfällen wirksam entgegenzutreten. Denn der Großteil von Sicherheitsvorfällen wird durch die Mitarbeitenden des Unternehmens gemeldet. Lediglich ein Bruchteil aller Meldungen wird davon durch Systeme wie Firewalls, Virenscanner o. Ä. erfasst.

In dieser Masterarbeit werden zwei Fallstudien ausgiebig analysiert. Dabei zeigt sich, dass gerade Ransomware ein lukratives Geschäftsmodell für Cyberkriminelle darstellt. Diese Art von Cyberangriff kann ein unvorbereitetes Unternehmen in eine prekäre Lage versetzen, in der es gewzungen wird, das Lösegeld zu zahlen, um wieder an seine entschüsselten Daten zu kommen.

Der Aufwand für Personen mit maliziösen Absichten, Cyberangriffe durchzuführen, hat sich über die Jahre deutlich reduziert. Diese können heutzutage auf automatisierte Tools und Konzepte wie Ransomware-as-a-Service (RaaS) zurückgreifen. Dadurch wird es selbst weniger technisch versierten Personen ermöglicht, Open-Source-Tools zu nutzen und auf frei verfügbares Wissen zurückzugreifen und dies für ihre bösartigen Absichten einzusetzen. Insbesondere deshalb ist die Anzahl der Cyberangriffe innerhalb der letzten Jahre deutlich angestiegen und ein Ende dieses Trends nicht in Sicht. Daher ist es lediglich eine Frage der Zeit, wann man Opfer eines solchen Angriffs wird und weniger, ob dies überhaupt geschehen wird.

Studien zeigen auf, dass hierbei gerade die organisierte Kriminalität zugenommen hat und zu den Betroffenen Unternehmen häufig die Kritische Infrastrukturen (KRITIS) gehören, wo neben dem Finanzwesen und dem Staat, ebenfalls Energiedienstleister zählen. Cyberangriffe auf Unternehmen hinterlassen hierbei deutlich ihre Spuren: So konnten im Vergleich zu 2020 im Jahr 2021 noch weniger Daten nach einem Cyberangriff (Ransomware) wiederhergestellt werden (5% weniger). Zudem befinden sich Energiedienstleister auf Platz zwei der Branchen, welche am meisten Lösegeld an die Erpresser gezahlt haben. Im Jahr 2021 entstand der deutschen Wirtschaft ein finanzieller Schaden von ca. 223 Mrd. Euro.

Incident Response Management stellt eine organisatorische Sicherheitsmaßnahme zur Krisenbewältigung dar, welche das Ziel verfolgt, einen

Prozess zu etablieren, worüber im Falle eines Sicherheitsvorfalls (Incidents) dieser frühestmöglich erkannt, eingedämmt und bekämpft werden kann. Erst dadurch können die Auswirkungen des Schadensausmaßes eines Incidents weitestgehend reduziert werden. Sowohl aus finanzieller (monetär), als auch technologischer (Systeme und Daten) und gesellschaftlicher Sicht (Ruf, Image & Vertrauen der Kunden). Zu den Sicherheitsvorfällen zählen unter anderem Malware, Datenschutzverletzungen und Cyberangriffe auf die IT-Infrastruktur eines Unternehmens.

Innerhalb eines solchen Konzepts werden dabei sowohl klare Verantwortlichkeiten, klare Abläufe als auch klare Kommunikationswege definiert. Über die Verantwortlichkeiten werden eindeutige Zuständigkeiten im Sinne von Rollen definiert. Die Mitglieder eines solchen Teams zur Bekämpfung von Sicherheitsvorfällen haben eindeutige Aufgabenbereiche für die sie zuständig sind. Die Abläufe werden als Prozesse abgebildet, welche alle notwendigen Schritte zur Erkennung, Analyse, Eindämmung, Wiederherstellung und Berichterstattung im Falle eines Incidents definieren. Über klare Kommunikationswege können alle relevanten Personenkreise schnellstmöglich über den Vorfall informiert und regelmäßig über neue Informationen benachrichtigt werden. Dies dient außerdem dem Zweck der Transparenz gegenüber Kunden und Partnern der CURSOR Software AG.

Cyberattacken stellen für alle Betroffenen Personen eine nicht zu unterschätzende Stresssituation dar. Dass ein Angriff jederzeit und ohne Vorwarnung eintreten und in kürzester Zeit immensen Schaden anrichten kann, treibt das Stresslevel der Verantwortlichen weiter in die Höhe. Ein Sicherheitskonzept, welches regelt, wie in Situationen von Sicherheitsvorfällen zu reagieren und kommunizieren ist, welches gleichzeitig eindeutige Verantwortlichkeiten und Abläufe definiert, kann das Stresslevel maßgeblich positiv beeinflussen und verhindert darüber hinaus die Notwendigkeit zur Improvisation. Dadurch können voreilig getroffene und unbedachte Reaktionen verhindert werden.

Diese drei Bereiche der klaren Verantwortlichkeiten, Abläufe und Kommunikationswege ermöglichen gemeinsam eine strukturierte und koordinierte Herangehensweise für die Bewältigung von Sicherheitsvorfällen im Rahmen des Incident Response Managements.

Mit dieser Masterthesis wird ein Incident-Management- & Response-Konzept für die CURSOR Software AG erstellt. Ein fester Bestandteil davon wird die Erstellung eines Prozesses sein, um zu definieren, wie auf mögliche Sicherheitsvorfälle zu reagieren und kommunizieren ist. Angefangen mit der Identifikation eines Vorfalls, über die Herangehensweise und Kommunikation (sowohl intern als auch extern (Kunden, Partner, usw.)) bis hin zur Retrospektive zur kontinuierlichen Verbesserung des Prozesses. Hierfür wird die interne Struktur der CURSOR Software AG und deren Anforderungen intensiv analysiert. Zugleich werden verschiedene Sichtweisen betrachtet: Öffentlich erreichbare Cloud-Instanzen, die interne und externe IT-Infrastruktur und Applikationen (z. B. das webbasierte CRM-System der CURSOR Software AG).

Literatur

Kappes, Martin (2022): Netzwerk- und Datensicherheit: Eine praktische Einführung, Springer Vieweg

Kaschner, Holger (2020): Cyber Crisis Management: Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation, Springer Vieweg

Knebelsberger, Uwe; Naefe, Arthur; Oelmaier, Florian (2023): Krisenfall Ransomware: Strategien für Wiederaufbau, Forensik und Kommunikation, Springer Vieweg

Königs, Hans-Peter (2017): IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken, Springer Vieweg

Schläger, Uwe; Thode Jan-Christoph (Herausgeber) (2022): Handbuch Datenschutz undd IT-Sicherheit, Erich Schmidt Verlag

Schuh, Günther; Zeller, Violett; Stich, Volker (Herausgeber) (2022): Digitalisierungs- und Informationsmanagement: Handbuch Produktion und Management 9, Springer Vieweg