Informationssicherheitsvorfälle

Vorfälle kommen in jedem Unternehmen vor. Sei dies durch eigene Personen, oft durch Unwissenheit oder durch externe Bedrohungen wie Hacker. Wichtig ist es, einen Vorfall schnell zu erkennen und die richtigen Schritte einzuleiten. Das Kapitel A.16 hat zum Ziel, «eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschliesslich der Benachrichtigung über Sicherheitsereignisse und Schwächen sicherzustellen».

Praktisch jeden Tag erscheinen in den Medien Berichte von Sicherheitsvorfällen. Produktionsausfälle und Schäden in die Millionen können die Folgen sein. Jedes Unternehmen kann betroffen sein, unabhängig von der Grösse oder Art des Unternehmens. Daher gilt es in einem ersten Schritt die Verantwortlichkeiten und Verfahren zu definieren. In vielen Firmen gibt es bereits ein Ticket-System. Dieses kann ideal mit dem Typ «Informationssicherheitsvorfälle» erweitert werden. Im Prozess sollte definiert sein, dass solche Vorfälle umgehend an die zuständige Person gelangen, zum Beispiel den CISO. Weiter gilt es im Vorfeld Verfahren zur Überwachung, Erkennung und Analyse schriftlich zu definieren. Ist bereits ein Monitoring vorhanden, sollten die Sensoren so trainiert werden, dass Anomalien einen Alarm auslösen. Zu Beginn ist mit vielen Fehlalarmen zu rechnen, mit der Zeit können diese eingedämmt werden. Tritt ein Vorfall ein, müssen die Schritte sauber protokolliert werden, damit diese auch rechtlich verwendet werden können.

Erkennung

Die eigenen Mitarbeitenden sind eine gute Quelle für die Erkennung von Vorfällen. Im Unternehmen sollte eine offene Kultur für Fehler existieren. Niemand soll Angst haben, Fehler zu melden. In der Norm wird explizit von unwirksamen Sicherheitsmassnahmen, Verstösse, menschliches Versagen, Nichteinhaltung von Richtlinien, unkontrollierte Systemänderungen, Fehlfunktionen und Zugangsverstösse geschrieben. Dürfen Abweichungen gemeldet werden, ohne mit negativen Folgen zu rechnen, können diese schnell angegangen und korrigiert werden. Auf welchem Weg dies geschieht, muss im Vorfeld definiert werden. Dies kann via ein Ticket sein, per Telefon oder E-Mail, aber auch Whistle Blowing sollte ermöglicht werden.

Beurteilung

Nach der Meldung oder der Erkennung eines Informationssicherheitsereignisses sollte dieses beurteilt werden. Dies ist gar nicht so einfach. Vermutlich müssen im Vorfeld weitere Informationen gesammelt werden, um ein Gesamtbild zu bekommen. Die Klassifizierungsrichtlinie sollte berücksichtigt werden. Je nach Art der Information gilt es anders vorzugehen. Sollte das Unternehmen ein Information Security Incident Response Team (ISIRT) haben, sollte dies möglichst früh einbezogen werden.

Ein Informationssicherheitsvorfall kann beispielsweise wie folgt klassifiziert werden:

- Sicherheitsschwachstelle oder Ereignis – es ist kein Vorfall aufgetreten, jedoch könnte das mit einem System, Prozess oder einer Organisation in Zusammenhang stehende Ereignis in naher oder ferner Zukunft einen Vorfall zur Folge haben
- Geringer Vorfall – ein Vorfall, der keine bedeutende Auswirkung auf die Vertraulichkeit oder Integrität von Informationen haben und keinen längerfristigen Ausfall der Verfügbarkeit verursachen kann
- Erheblicher Vorfall – ein Vorfall, der erheblichen Schaden durch den Verlust der Vertraulichkeit oder Integrität von Informationen verursachen kann oder der eine Unterbrechung der Verfügbarkeit von Informationen und/oder Prozessen über eine inakzeptable Zeitspanne verursachen könnte
- Datenschutzverletzung – ein Vorfall, der rechtliche Folgen in Bezug auf den Datenschutz haben kann. Dies muss unabhängig von der Schwere des Vorfalls gemeldet werden.

Bei einer Datenschutzverletzung lässt die DS-GVO grüssen. Sind schützenswerte Daten betroffen, müssen die Kundinnen und Kunden und eventuell gar die Datenschutzaufsichtsbehörde informiert werden. Auch in der Schweiz sollte je nach Schwergrad der EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeits-Beauftragter) konsultiert werden. Die Dringlichkeit eines Vorfalls kann wie folgt kategorisiert werden:

- Gering: Der vom Vorfall verursachte Schaden nimmt im Verlauf der Zeit nur unwesentlich zu. Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nicht zeitkritisch.
- Mittel: Der vom Vorfall verursachte Schaden nimmt im Verlauf der Zeit substanziell zu. Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nur mässig zeitkritisch. Einzelne Benutzer sind betroffen.
- Hoch: Der vom Vorfall verursachte Schaden nimmt im Verlauf der Zeit schnell zu. Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind sehr zeitkritisch. Durch schnelles Handeln kann verhindert werden, dass aus einem hohen ein kritischer

Bild: Archiv

Nach der Meldung oder der Erkennung eines Informationssicherheitsereignisses muss gehandelt werden.

Vorfall wird. Mehrere Benutzer sind betroffen.
– Kritisch: Der vom Vorfall verursachte Schaden nimmt im Verlauf der Zeit schnell zu. Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind wichtig. Zudem sind viele Benutzer betroffen.

Massnahmen

Der nächste Schritt ist das Ergreifen von vorher definierten Verfahren und Abläufen. Alle Informationen sollten frühzeitig gesichert werden. Allenfalls kommen forensische Analysen dazu. Suchen Sie dazu im Vorfeld einen geeigneten Partner. Dieser weiss, wie vorgegangen werden muss, damit Spuren auch vor Gericht standhalten. Es gilt auch eine mögliche Eskalation im Auge zu behalten. Welche Partner und Lieferanten sind mit einzubeziehen? Welche internen und externen Personen müssen kontaktiert werden? Für die Kommunikation ist im Vorfeld eine Person zu bestimmen. Nur diese darf gegen innen und aussen kommunizieren. Das Redeverbot für alle anderen ist wichtig, damit nicht falsche Aussagen oder Gerüchte kursieren.

Jeder Schritt, der getroffen wird, gilt es zu protokollieren. Und dies nicht erst im Nachhinein, sondern laufend. Schon einen kurzen Moment später ist in der Hektik nicht mehr jeder Schritt klar. Das Sammeln von Beweismaterial sollte ebenso im Vornherein definiert werden. In welcher Art und Form wird protokolliert? Wie werden die Informationen gesammelt und sicher aufbewahrt?

Nachbearbeitung

Nach dem Sicherheitsverstoss gilt es alles aufzuarbeiten. Welche Erkenntnisse können gezogen werden? Welche Kosten sind bei der Behebung entstanden? Sind indirekte Kosten wie ein Vertrauensverlust zu erwarten? Wie kann ein solcher Vorfall in Zukunft vermieden werden? Welche Massnahmen gilt es noch zu ergreifen? Jeder Vorfall hilft, die Informationssicherheit weiter zu verbessern. Meine Auditoren-Erfahrung zeigt, wenn offen über einen Vorfall informiert wird, melden sich weitere Personen, die etwas Ähnliches gesehen haben oder wissen. Zum Beispiel bei einem Einbruch kommen allenfalls weitere Schwächen zum Vorschein, die sonst «verschwiegen» wurden.

Fazit

Das frühzeitige Erkennen und das Treffen von richtigen Schritten kann einen Informationssicherheitsvorfall positiv beeinflussen und mögliche negativen Folgen reduzieren. Das Vorgehen gilt es im Vorfeld zu definieren und regelmässig zu üben. Mit dem Wissen und der Erfahrung können Ereignisse verhindert oder mindestens die Folgen reduziert werden.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch