Wer macht was, wann und warum?

Höhere Gewalt wie Naturkatastrophen, menschliche Eingriffe von außen in Form von Cyberangriffen oder von innen, beispielsweise durch Spionage oder Sabotage von Mitarbeitenden – all das gefährdet Organisationen und kann zu erheblichem Schaden führen. In einer Krisensituation greifen im besten Fall die im Rahmen des Business Continuity Managements festgelegten Strategien und Maßnahmen.

Text: Alexander Vogel

Aber wie viel Schutz braucht ein Unternehmen, welche Geschäftsprozesse sind besonders gefährdet und welche sollten in einer Notsituation als Erstes geschützt werden? Und mehr noch: Was bedeutet eigentlich „geschützt“ und wie werden relevante Prozesse und Assets schnellstmöglich wieder funktionstüchtig?

Um Fragen wie diese nicht willkürlich aus dem Bauch heraus zu beantworten, setzen sich Experten mit der Organisation und ihren Produktionsstätten auseinander. Sie analysieren, welche Prozesse und welche Assets kritisch für das Unternehmen sind und welchen Risiken diese ausgesetzt sind.

Für die Wahrung der Schutzziele der Informationssicherheit werden innerhalb einer Schutzbedarfsanalyse sowie der anschließenden Gefährdungs- und Risikoanalyse ermittelt, was die unternehmenskritischen und -wichtigen Prozesse und Assets sind und welchen Gefährdungen und Risiken diese unterliegen. Darauf aufbauend werden Prozesse zur Organisation im Krisenfall entwickelt.

Über den Autor Alexander Vogel

Alexander Vogel ist Senior Berater für den Bereich Datenschutz und seit über zehn Jahren für die DATATREE AG tätig. Seine Schwerpunkte umfassen die Projektleitung in den Bereichen der medizinischen Informationssysteme sowie Datenschutzprojekte von Großkunden im Gesundheitswesen.

DIE SCHUTZBEDARFSANALYSE

Die Schutzbedarfsanalyse ist der Start für Informationssicherheitsbeauftragte, um herauszufinden, welche Prozesse in einer Organisation Schutz benötigen und wie hoch ihr Schutzbedarf jeweils sein sollte. Sie ist die Grundvoraussetzung für die darauffolgende Gefährdungs- und Risikoanalyse.

DIE HERANGEHENSWEISE: TOP-DOWN VS. BOTTOM-UP

Grundsätzlich gibt es zwei unterschiedliche Herangehensweisen, die in ihren Wirkungsrichtungen unterschiedlich sind: Top-Down oder Bottom-Up. Gehen Experten „von unten nach oben“ - also Bottom-Up, nehmen sie zunächst kleinste Assets unter die Lupe, wie beispielsweise den Laptop mit der Inventarnummer 4711, und arbeiten sich dann in höhere Hierarchien vor, bis sie zum Beispiel im Prozess der Befundung einer CT-Untersuchung angelangt sind. Voraussetzend und gleichzeitig nachteilig für dieses Vorgehen ist, dass im Vorfeld eine Liste mit allen Assets vorhanden sein muss. Die Erstellung ist oft mühsam, zeit- und ressourcenaufwendig.

Der Top-Down-Ansatz geht genau umgekehrt vor: Experten beginnen auf Prozessebene, also einem übergeordneten Ziel und arbeiten sich dann weiter nach unten zu einzelnen Assets vor. Dies birgt die Vorteile, dass ein Assetmanagement nach und nach aufgebaut werden und das Risikomanagement in Form der Schutzbedarfsanalyse zeitnah starten kann. Ebenfalls führt der Top-Down-Ansatz zu einer prozessorientierten Risikobetrachtung.

WAS HEISST EIGENTLICH „SCHUTZ“?

Das Ziel, ein Unternehmen zu schützen, klingt erst einmal einleuchtend. Was genau aber muss und kann geschützt werden? Genauer betrachtet ist der Begriff “Schutz” sehr abstrakt, nicht eindeutig definierbar und schon gar nicht ganzheitlich überprüfbar. Und um es noch komplizierter zu machen: Was tatsächlich geschützt werden muss, ist organisationsabhängig. Für wirtschaftsorientierte Unternehmen sind insbesondere finanzielle Auswirkungen existenziell, hier ist besonders der Schutz von Assets oder Prozessen relevant, bei denen im Schadensfall hohe Kosten entstehen. Für Behörden hingegen ist häufig die Reputation von hoher Bedeutung und schützenswert, damit sie möglichst nicht angekratzt wird. One size fits all - in der Schutzbedarfsdefinition gibt es das nicht.

Um den tatsächlichen Schutz besser einordnen zu können und greifbar zu machen, wurden Schutzziele definiert, die einzelne Einheiten in einer Organisation eingrenzen. In der Informationssicherheit stehen besonders drei Schutzziele im Fokus: Vertraulichkeit, Integrität und Verfügbarkeit. Je nach Anforderung gibt es weitere Schutzziele, wie beispielsweise Authentizität, Zurechenbarkeit oder Verbindlichkeit. Im Gesundheitswesen werden auch Schutzziele wie Patientensicherheit und Behandlungseffektivität definiert. Die Entscheidung, welche Schutzziele innerhalb der Schutzbedarfsanalyse herangezogen werden, ist wiederum von der Organisationsstruktur abhängig und wird je nach Bedarf entschieden.

Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gelten allerdings als Grundwerte und sollten innerhalb der Schutzbedarfsanalyse immer abgedeckt sein.

VERTRAULICHKEIT

Es ist so naheliegend wie relevant: Nur befugte Personen dürfen vertrauliche Informationen einsehen, bearbeiten und verwalten. Unter dem Schutzziel der Vertraulichkeit wird von Informationssicherheitsexperten entsprechend überprüft und festgelegt, wer welche Informationen einsehen und bearbeiten darf und welche Maßnahmen - beispielsweise Verschlüsselung - getroffen werden müssen, damit Unbefugte keinen Zugriff haben.

INTEGRITÄT

Informationen müssen verlässlich sein und bleiben. Unter dem Schutzziel der Integrität fallen daher alle Maßnahmen, die dazu beitragen, die Unversehrtheit von Daten sicherzustellen. Werden Informationen verändert, ist es wichtig, die Änderungen nachvollziehen zu können.

VERFÜGBARKEIT

Das Schutzziel Verfügbarkeit bezieht sich auf die gesamte Dauer, in der die Systeme im Unternehmen funktionieren, also verfügbar sind. Im Rahmen der Risikoanalyse wird unter diesem Schutzziel erörtert, welche Systeme oder Daten verfügbar sein müssen, damit das Unternehmen trotz Krisenfall im Betrieb bleibt.

Sind die Schutzziele definiert, beschäftigen sich Experten mit der Frage: Wie hoch ist der Schutzbedarf? Das Bundesamt für Sicherheit und Informationstechnik (BSI) empfiehlt deshalb drei Schutzbedarfskategorien, die einen potenziellen Schaden zunächst folgendermaßen einordnen:

NORMAL	Die Schadensauswirkungen sind begrenzt und überschaubar.
HOCH	Die Schadensauswirkungen können beträchtlich sein.
SEHR HOCH	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.[1]

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_01/Lektion_4_01_node.html

Wann ein Asset oder ein Prozess einen normalen, hohen oder sehr hohen Schutzbedarf hat, ist auch hier wieder von der Organisation abhängig und muss individuell betrachtet werden: Während ein finanzieller Schaden von bis zu 100.000 Euro für einen Großkonzern überschaubar sein kann, ist er für ein mittelständisches Unternehmen unter Umständen existenzbedrohend. Informationssicherheitsexperten müssen also auch hier von Fall zu Fall abwägen, welche Schutzbedarfskategorie zutrifft. Die Schutzbedarfsanalyse ist abgeschlossen, wenn alle zu bewertenden Assets und Prozesse auf die definierten Schutzziele hin überprüft und bewertet wurden.

DIE GEFÄHRDUNGS- UND RISIKOANALYSE:

Die Gefährdungs- und Risikoanalyse beginnt zunächst mit der Betrachtung derjenigen Prozesse oder Assets, die in der vorangegangenen Schutzbedarfsanalyse in die Kategorie „sehr hoch“ gefallen sind. In einem späteren Schritt folgt auch die Betrachtung der mit „hoch“ bewerteten Prozesse oder Assets.

Das BSI empfiehlt die Erstellung eines Gefährdungskatalogs. In diesem werden zunächst Szenarien kreiert, um zu betrachten, welche Prozesse bzw. Assets einer Gefährdung ausgesetzt sind. Stehen beispielsweise die Server eines Krankenhauses im Keller und liegt das Krankenhaus in der Nähe eines Flusses, wird das Szenario „Hochwasserkatastrophe durch Starkregen“ betrachtet. Jedem Szenario wird somit eine eigene Risikogefährdung zugeordnet. Im genannten Beispiel ist die Risikogefährdung hoch. Läge das Krankenhaus fern von Wasser, wäre die Gefährdung entsprechend niedrig. Auf diese Weise kann dann die Eintrittswahrscheinlichkeit für das potenzielle Risiko bewertet werden, mit der die Gefährdung tatsächlich eintritt.

In der hieraus resultierenden Risikobehandlung wird schließlich die Frage beantwortet: Was soll im Falle einer Gefährdung passieren?

Die Risikobehandlung wird in der Regel
in folgende Klassen unterteilt:
• AKZEPTANZ • MINDERUNG • ÜBERTRAGUNG • VERMEIDUNG

Denn hierauf kommt es schließlich an: Kann und muss das Risiko im Vorfeld vermieden werden? Ist das Risiko so hoch, dass es reduziert werden muss – und wenn ja, wie? Oder kann ein Risiko sogar akzeptiert werden? Wird beispielsweise dem Geschäftsprozess „Server Betrieb“ der Verlust von Hardware mit dem Risiko „mittel“ bewertet, so fällt die Entscheidung hier möglicherweise auf „Risikoakzeptanz“ und es müssen keine Ressourcen in Maßnahmen fließen, um das Risiko auszuschließen. Für die Akzeptanz gibt es wiederum „Risikoakzeptanzkriterien“, die für jede Organisation individuell ausfallen und im Vorfeld bestimmt werden. Fällt beim Geschäftsprozess „IT-Wartung“ das Szenario „Personalausfall“ in die Risikogruppe der Kategorie „sehr hoch“, so wird die darauffolgende Entscheidung „Risikominderung“ entsprechende Strategien - beispielsweise Personalaufbau - erfordern, um dieses Risiko auf minimalem Niveau zu halten. Die vorgeschlagenen Maßnahmen werden dabei genau dokumentiert, ebenso wie das immer verbleibende Restrisiko.

Eine Risikoanalyse ist nicht in Stein gemeißelt und so wandelbar wie der Alltag in einer Organisation. Wenn neue Technologien in der Lage dazu sind, Cyberangriffe aggressiver in IT-Systeme eindringen zu lassen, nimmt das damit verbundene Risiko zu und der Schaden wird womöglich größer. Aus diesem Grund ist sie immer in einem gewissen Zyklus zu wiederholen und Prozesse und Assets sind immer wieder neu zu bewerten. Im Gesundheitswesen beispielsweise werden Gefährdungs- und Risikoanalysen jährlich wiederholt.

Fazit

Wer seine Organisation schützen möchte, sollte auf Prophylaxe statt auf Therapie setzen.

Die im Vorfeld durchgeführten Schutzbedarfs- sowie Gefährdungs- und Risikoanalysen kategorisieren ein Unternehmen in sinnvolle Einheiten und machen willkürliche und teilweise überteuerte Vorsorgemaßnahmen obsolet. Gleichzeitig schützen sie die Organisation kalkuliert und nachhaltig. Dabei hat jede Organisation individuelle Schwerpunkte und Schwachstellen und damit auch individuelle Risikoeigenschaften. Es gibt keine Einheitsmaßnahmen, deshalb lohnt es sich Experten zu engagieren, die mit einem geschulten Auge eine Organisation individuell auf ihre Risiken hin bewertet.

Möchten Sie wissen, wie gut Ihr Unternehmen im Krisenfall geschützt ist und was Sie optimieren können?

Die Informationssicherheitsexperten der DATATREE AG unterstützen Sie dabei. Wenden Sie sich hierzu gerne an: sales@datatree.ag