optimus amicus
GMBH

7 Schritte im Umgang mit kritischen Vorfällen

Speziell für Vorfälle in der Cybersicherheit

Vorwort

Ich freue mich, Ihnen in diesem Whitepaper ein Thema vorzustellen, welches mir persönlich am Herzen liegt.
Bereits in den vergangenen Jahren, wie auch dieses Jahr, stehen die Cyberbedrohungen auf den obersten Positionen der kritischen Vorfälle in Unternehmen.

Noch immer gibt es eine Vielzahl von Unternehmen, welche für Risiken, Ereignisse oder Bedrohungen keine Vorkehrungen treffen und diese schlicht ignorieren. Einigen der Leser mag vielleicht der Begriff «grey rhino» bekannt sein, welcher durch *Michele Wucker* geprägt wurde. Dieser sagt nichts anders aus wie, dass man etwas kommen sehen kann, aber nur wenn man auch hinschaut. Damit meine ich, dass man einen grundlegenden Teil von Risiken oder Bedrohungen für das Unternehmen erkennen kann, wenn man nur einfach richtig hinschaut.

Die Anzahl an Cyberangriffen hat im Jahr 2021 mit Vergleich zum Vorjahr massiv zugenommen und dies hat einschneidende Auswirkungen auf Sicherheitsvorfälle, welche die Situation verschärfen. Auch für das Jahr 2022 wird es nicht besser aussehen, die ersten wenigen Tage dieses Jahres deuten leider bereits unmissverständlich darauf hin.

Es sollte an oberster Stelle in den Prioritäten Ihres Unternehmens stehen, dass die Widerstandsfähigkeit und die Wiederanlaufzeit nach einem Vorfall, der alleinigen Schlüsselfaktor ist, um mit Ihrem Unternehmen solche Vorfälle zu überstehen.

Für die optimus amicus GmbH
Philip Helfenberger (Senior Consultant & Geschäftsführer)

Im Januar 2022

https://www.optimus-amicus.ch

Warum es elementar ist, ein Krisenmanagement aufzubauen

Von Unternehmen wird verlangt, dass diese schnell auf kritische Ereignisse reagieren, um die negativen Auswirkungen im Rahmen halten zu können. Doch nur selten werden die dazu nötigen Ressourcen zur Verfügung gestellt und ein Vorgehen bzw. einen Plan, wie es sich zu verhalten gilt, fehlt meist komplett. Dadurch ist es fast unmöglich auf solche Ereignisse genügend schnell und noch wichtiger in richtigem Mass und den passenden Massnahmen zu reagieren.

Vorfälle, welche den Betrieb stören, treten täglich auf. Nicht alle sind gleich Krisen, doch auf alle Vorfälle gilt es mit den richtigen Massnahmen zu reagieren. Solche Vorfälle können mit einem kurzen Stromausfall beginnen und über kleine Datenschutzverletzungen bis hin zu Cyberangriffen gehen, welche das ganze Unternehmen tagelang lahmlegen können.

Es ist zentral, dass Personen, welche für die Sicherheit zuständig sind, mehr Zeit bekommen und idealerweise auf Ressourcen von aussen zugreifen können. Solche Dienstleister können mit objektivem Fokus auf Risiken und mögliche Massnahmen hinweisen und unterstützen interne Kräfte bei einer optimalen Sicherheitslösung. Wenn es im Unternehmen noch nicht mal definierte Personen gibt, welche sich darum zu kümmern haben, ist es noch wichtiger hier ins Handeln zu kommen und entsprechen Personen zu definieren und Pläne zu verfassen.

Abb1: Flut von Fragen, die ein schnelles Handeln erfordern

Die TOP 5 der Bedrohungen in der Cyberangriff & Datenschutzverletzungen

1. Phishing

Was wird unter Phishing verstanden:
Phishing ist ein Hacking-Schema, das Benutzer dazu verleitet, in einer schädlichen Nachricht eine Aktion auszuführen. Die Phishing-Nachricht erscheint auf den ersten Blick wie eine normale E-Mail mit legitim aussehenden Links, Anhängen, Firmennamen und Logos. Die E-Mail überzeugt die Benutzer, Massnahmen zu ergreifen, sei es durch das Klicken auf einen Link oder das Herunterladen eines Anhangs. Eine Phishing-E-Mail kann auch eine Clickbait-Betreffzeile enthalten, die Ihre Aufmerksamkeit auf sich zieht. Eine erweiterte Form des Phishing ist das *Whale-Phishing*, dieses richtet sich an Führungskräfte von Unternehmen. Alternativ senden die Hacker bei einem *Spear-Phishing* die E-Mails an eine bestimmte Mitgliedergruppe eines Unternehmens, um Informationen zu stehlen. Dem gegenüber wird im «klassischen» Phishing keine Person oder Unternehmung targetiert, sondern die Nachricht wird an eine Vielzahl von E-Mail Empfängern geschickt. Möglicherweise stammen die E-Mail-Adressen aus einem Leak auf einer Internetplattform.

Was ist das Ziel:
Das Ziel von Phishing, egal in welcher Form, ist es, persönliche Informationen zu stehlen, die irgendwie gewinnbringend verwertet werden können.

Wie entwickelt sich die Situation:
In einer aktuellen Studie von Cisco – Trends der Cyber-Sicherheitsbedrohung 2021: Ist Phishing ganz oben auf der Liste – 86 % der Unternehmen gaben an, dass jeweils mindestens ein Benutzer auf das Phishing hereinfällt und die Aktion ausführt. Daher kann ein falscher Klick eines Mitarbeiters ein Unternehmen einem massiven Risiko aussetzen.

2. Malware

Was wird unter Malware verstanden:
Malware, ist eine bösartige Software, mit welcher die Geräte gehackt werden sollen. Malware installiert meist «Agenten» auf dem Computer, welche unter anderem als Trojaner, Spyware, Viren, Ransomware, Adware und Würmer bekannt sind.

Malware kann auf einen Computer übertragen werden, indem Sie auf einen infizierten Link klicken oder eine Datei von einer (unbekannten) Quelle herunterladen, auf eine Popup-Werbung klicken oder einen E-Mail-Anhang herunterladen. Die Quelle muss nicht immer unbekannt sein, es ist auch möglich, dass mittels einer Malware auf den E-Mail-Client (bspw. Outlook) Zugriff genommen wird und so Mails versendet werden, welche für den Empfänger nicht von einer unbekannten Person stammen.

Was ist das Ziel:
Sobald Malware in einem Computersystem festgesetzt hat, können Hacker Zugang zu den Passwörtern, Kreditkartennummern, Bankdaten, Personalakten, E-Mail-Verkehr und mehr Ihres Unternehmens erhalten.

Wie entwickelt sich die Situation:
Im letzten Jahr berichteten Unternehmen, dass 35 % aller Malware-Angriffe, auf die sie stiessen, bisher unbekannte Malware oder Methoden verwendeten. Leider wird dieser Prozentsatz wahrscheinlich steigen, da noch immer vermehrt Mitarbeiter aus der Ferne arbeiten.

3. Ransomware

Was wird unter Ransomware verstanden:
Ransomware ist eine spezielle Form von Malware, die die Computersysteme der Benutzer verschlüsselt. Sobald ein Ransomware-Angriff implementiert wurde, können Benutzer nicht mehr auf ihre Systeme oder Dateien zugreifen. Damit Benutzer wieder auf ihre Systeme zugreifen können, müssen sie den Cyberkriminellen ein Lösegeld zahlen.

Lösegeld Transaktionen werden oft über Bitcoin getätigt. Cyberkriminelle können auch andere Zahlungsmethoden anfordern, wie bspw. Amazon-Geschenkkarten. Das Lösegeld kann enorm schwanken und geht von einigen Hunderten bis zu Hunderttausenden von Dollar. Auch mit der Zahlung des Lösegelds ist nicht sicher, ob Sie dadurch wieder Zugriff auf ihre Systeme erhalten. Abzuwägen, ob ein Lösegeld bezahlt werden soll oder nicht, hängt sehr stark davon ab, wie gut Sie auf eine solche Situation bereits vorbereitet sind.

Was ist das Ziel:
Ransomware hat in erster Linie das Ziel, dass die Hacker-Gruppen an Geld kommen. Als ein weiterer Grund kann die Schädigung eines Unternehmens genannt werden, da durch Ransomware ein Betriebsunterbruch entsteht, welcher dem Unternehmen direkt Schaden zufügt.

Wie entwickelt sich die Situation:
Ransomware wird häufig durch einen Download von einer Webseite oder eines Anhangs in einem Mail verbreitet. Ein Angriff kann sowohl auf einzelne Mitarbeiter als auch auf ganze Organisationen abzielen. Während der Pandemie meldeten beachtliche 58 % der Unternehmen Umsatzeinbussen als direkte Folge eines Ransomware-Angriffs.

4. Datenschutzverletzungen

Was sind Datenschutzverletzungen:
Eine Datenschutzverletzung tritt auf, wenn sensible Daten ohne Genehmigung des Datenurhebers aus einem System gestohlen werden. Vertrauliche Informationen können unter anderem Kreditkartennummern, Sozialversicherungsnummern, Namen, Privatadressen, E-Mail-Adressen, Benutzernamen und Passwörter umfassen.

Sicherheitsverletzungen können durch einen Angriff auf das System erreicht werden. Als Beispiel kann ein Angriff auf die Netzwerkinfrastruktur gestartet werden, wenn die Cyberkriminelle eine Schwachstelle erkennen und diese dann ausnutzen, um in das System einzudringen. Auch Social Engineering ist weit verbreitet. Mittels Social Engineering soll möglichst viel über eine Person in Erfahrung gebracht werden, um diese mittels psychologischer Manipulation dazu zu bringen, Zugriff zu einem System zu gewähren oder vertrauliche Informationen herauszugeben. Sie können bspw. dazu verleitet werden, einen schädlichen Anhang herunterzuladen oder Anmeldeinformationen zu einem System preiszugeben.

Was ist das Ziel:
Die Absichten hinter den vielfältigen Datenschutzverletzungen sind sehr vielfältig und reichen von Sabotage über monetären Antrieb bis zu Spionage.

Wie entwickelt sich die Situation:
Laut einer Datenschutzverletzungsanalyse des Identity Theft Resource Center (ITRC) sind die öffentlich gemeldeten Datenschutzverletzungen in den USA im zweiten Quartal 2021 um 38 % gestiegen.

5. Kompromittierte Passwörter

Was sind kompromittierte Passwörter:
Kompromittierte Passwörter treten am häufigsten auf, wenn ein Benutzer seine Zugangsdaten unwissentlich auf einer gefälschten Website eingibt. Häufige Kombinationen aus Benutzername und Kennwort machen Konten ausserdem anfälliger für Angriffe. Die Verwendung von gleichen Passwörtern über mehrere Plattformen hinweg erhöht die Gefahr noch zusätzlich, da ein anfälliger Hacker mit den gleichen Kombinationen zu mehreren Konten Zugriff erhalten kann.

Was ist das Ziel:
Durch kompromittierte Passwörter entsteht meist ein Datenschutzproblem, da die Hacker Zugriff auf vertrauliche Unternehmensdaten erhalten können. Mit diesen Daten können sie einen Erpressungsversuch starten, diese an konkurrierende Unternehmen verkaufen oder die Daten nutzen, um weitere Angriffe gegen ein Unternehmen zu starten.

Wie entwickelt sich die Situation:
Stellen Sie beim Erstellen von Passwörtern für Firmenkonten immer sicher, dass Sie eindeutige, schwer zu erratende Passwörter verwenden. Da 51 % der Personen angeben, dass sie sowohl für ihre geschäftlichen als auch für ihre privaten Konten dieselben Passwörter verwenden, weisen Sie Ihre Mitarbeiter an, spezifische Richtlinien für maximale Sicherheit zu befolgen.

1. EINEN PLAN ERSTELLEN

Es scheint auf den ersten Blick nicht so schwer zu sein, einen Plan zu erstellen, jedoch muss dieser umfassend sein, damit er wirklich effektiv ist.
Als Erstes wird ein grundlegender Plan erstellt, welcher dann für die jeweilige Krise erweitert und verfeinert wird. Damit wird erreicht, dass in unterschiedlichem Umfang auf verschiedene Bedrohungen reagiert werden kann. Diesen Aufgaben werden Ressourcen und Massnahmen zugeordnet.

Angesichts der Arten von Bedrohungen, welchen Ihr Unternehmen ausgesetzt sein kann, sollte folgendes bedacht werden:

++ Kritische Ereignisse sollen angemessen nach deren Art, Auswirkung und Ausmass kategorisiert werden. Dabei ist zwischen Routinevorfällen und Krisenereignissen zu unterscheiden.

++ Legen Sie fest, wie die Organisation mit einem Ereignis umgeht und definieren Sie klar, wer die Führung übernimmt.

Der Plan sollte Abstufungen für die Schweregrade enthalten, welche die Basis für die Zusammenstellung der Teams zur Bewältigung des Ereignisses sein solle.
Wenn Ihr Unternehmen bereits über Pläne für ein Krisenmanagement verfügt, stellen Sie bitte regelmässig sicher, dass diese in betriebsbereitem Zustand sind, sprich stets aktuell und auch regelmässig der aktuellen Situation angepasst. Nicht selten sind in solchen Plänen noch Mitarbeiter vermerkt, welche das Unternehmen bereits vor einiger Zeit verlassen haben, dies ist natürlich gelinde gesagt suboptimal, gerade wenn es sich noch um eine Person handelt, welche in einer führenden Rolle sich um die Krise hätte kümmern sollen.

Ebenfalls muss die Verfügbarkeit der Pläne jederzeit und auch für jegliche Krisen sichergestellt sein. Stellen wir uns vor, die Pläne sind digital auf einem Server abgelegt und die Krise ist eine Verschlüsselungsattacke, welche sämtliche Daten auf dem Server verschlüsselt hat. Dann bringt dieser Plan nicht mehr viel, da ein Zugriff auf diesen schlicht nicht mehr möglich ist. Das muss unbedingt berücksichtigt werden und es müssen Kopien, auch auf anderen Medien bspw. Papier, vorhanden sein.

Die Unterscheidung zwischen „Alltags-" und „Krisen-" Notfällen sollte Ihre Reaktionsstrategie beeinflussen. Eine Alltagsnotfall bedeutet nicht, dass man darauf mit «kein Problem» reagieren soll. Im Gegenteil, alltägliche Notfälle können sehr schwierig und herausfordernd sein. Die Alltäglichkeit bezieht sich mehr auf die mögliche Vorhersehbarkeit der Situation, was eine gute Vorbereitung verlangt. Das von dieser Situation ausgehende Risiko wurde in Ihren Reaktionsplänen aufgenommen und Sie haben wahrscheinlich entsprechende Abläufe und Schulungen dazu definiert und durchgeführt. Kurz gesagt, Ihre Geschäftskontinuität ist mittels Incident Response und Disaster Recovery Plänen vorbereitet und die Strategien zu deren Umgang sind klar.
Im Gegensatz dazu ist ein «Krisen-Notfall» ein ganz anders Thema. Diese Vorfälle zeichnen sich dadurch aus, dass immer eine Komponente des unerwarteten bzw. eine ganz neue Gegebenheit eintritt. Die unerwartete Komponente macht es dann eben auch so schwierig richtig darauf zu reagieren.

Eine solche Art von Notfall hat meistens eine oder mehrere der folgenden Eigenschaften.

1. Die Bedrohungen sind so noch nie aufgetreten, d. h., es gibt keinen Plan und Massnahme, wie darauf zu reagieren ist.
2. Die Situation kann ein bekanntes Ereignis sein, entwickelt sich jedoch in noch nie dagewesener Geschwindigkeit, was einer angemessenen Reaktion (inklusive Benachrichtigung / Koordination) komplett entgegenwirkt und es zu einer grossen Herausforderung macht.
3. Der Vorfall erhält eine ganz neue Dimension, in dem mehrere Faktoren, welche einzeln noch kontrollierbar waren, in diesem Ereignis nun kombiniert auftreten und so ganz neue Auswirkungen an den Tag legen können. In dieser neuen Kombination stellt dieses Ereignis eine einzigartige Herausforderung dar.

Mit Fokus auf Cybersicherheit sind die folgenden Punkte relevant und können mit in die Planung einbezogen werden.

1. Bauen Sie Fachwissen auf – intern und/oder extern

Verschiedene Unternehmen, insbesondere kleine und mittlere Unternehmen, haben möglicherweise Schwierigkeiten, das richtige Team zu besetzen, um sicherzustellen, dass ein Unternehmen vor den neuesten Cyber-Bedrohungen geschützt und bereit ist, Angriffe abzuwehren. Die Einstellung eines IT-Security Officer kann teuer sein, und wenn Sie nicht bereits über das Fachwissen im Haus verfügen, kann es schwierig sein, die fachlichen Fähigkeiten einer solchen Person einzuschätzen.

Viele Unternehmen entscheiden sich dafür, Cybersicherheit als Mandat an externe Unternehmen zu erteilen. Zwei Vorteile, die sich in der Zusammenarbeit mit einer externen Organisation ergeben sind, dass sie rund um die Uhr Zugang zu Experten haben und sich auf einen hohen Praxisbezug der Personen verlassen können, da diese genau in dem Bereich ihr Wissen und Erfahrungen haben. Gerade in dem Erstellen von Konzepten und Plänen, ist es enorm wichtig, mit Personen zusammenzuarbeiten, welche eine langjährige Erfahrung im Verfassen solcher Pläne haben. Das Einschätzen von passenden Massnahmen und die Definition von Abläufen erfordern eine vorhandene Erfahrung, anders ist dies ein reines «Rätselraten», was selten von Erfolg gekrönt sein wird.

2. Bilden Sie Ihre Mitarbeiter aus

Eine der besten Cybersicherheitspraktiken ist die Schulung von Mitarbeitern. Dies mag für die meisten offensichtlich erscheinen, aber trotzdem besteht hier noch immer in vielen Unternehmen ein grosser Handlungsbedarf. Es ist sehr wichtig, die Mitarbeiter in diesen Themen zu schulen, um sicherzustellen, dass alle auf dem gleichen Stand sind. Sprechen Sie mit Mitarbeitern über die Bedeutung starker Passwörter, wie Sie die IT-Infrastruktur sicher verwenden und welche Richtlinien für die Internetnutzung und den Umgang damit gelten. Dies alles zum Schutz der Mitarbeiter, Ihres Unternehmens und Ihrer Kunden.

Schulen Sie Ihr Team darin, Phishing-Angriffe zu erkennen, indem Sie ein Bewusstsein dafür schaffen und aufzeigen, wie solche zu erkennen sind. Erklären Sie Ihren Mitarbeitern, warum niemals nach Passwörtern oder der gleichen gefragt wird und warum es besonders wichtig ist, mit persönlichen Informationen vorsichtig umzugehen. Ihre Mitarbeiter können so einen wertvollen Beitrag zur allgemeinen Informationssicherheit Ihres Unternehmens beitragen.

3. Erstellen Sie für die häufigsten Cyberangriffe einen Plan

Für die wahrscheinlichsten Angriffe auf Ihr Unternehmen, sollten Sie einen Plan erstellen, wie Sie darauf reagieren wollen. Ein solches Dokument muss lebendig sein, das mit jeder neuen Erkenntnis und der Reaktion darauf verbessert werden kann. Aus solchen Dokumenten können auch neue Anforderungen an die Systeme abgeleitet werden, sodass Ihre Infrastruktur in Zukunft noch sicherer wird.
Ein Incident Response Plan (IRP) als Teil Ihres Business Continuity Managements (BCM) ist ein wichtiges Puzzleteil einer guten Vorbereitung auf die aktuellen Gefahren in der Cybersicherheit. Es ist blauäugig auf diese Gefahren mit nichts Tun zu reagieren. Aktuell gilt die Devise nach wie vor: «Es ist nicht eine Frage, ob Sie angegriffen werden, sondern nur noch die Frage, wann Sie angegriffen werden.» Diese Wahrheit ist nicht schön, doch es hilft auch nichts, sich dieser zu verschliessen.

Ihre IRP's sollten Ihren Mitarbeitern leicht zugänglich sein und regelmässig überprüft werden, um sicherzustellen, dass die gesamte Organisation bzw. die beteiligten Personen den Prozess verstehen und diesen auch einhalten können.

Ein Plan, der gründlich ausgeführt und regelmässig überprüft wird, ist der beste erste Schritt, um die Sicherheit von Unternehmens- und Kundeninformationen zu gewährleisten. Unabhängig davon, ob Sie internes Know-how aufbauen oder einen vertrauenswürdigen externen Partner finden, Cybersicherheit kann kein Projekt mehr sein, das auf Eis gelegt wird. Das Verständnis der neuesten Bedrohungen und der Massnahmen, um deren Auswirkungen auf Ihr Unternehmen zu verhindern, ist der Schlüssel zum Schutz Ihres Unternehmens.

2. AUFBAU EINES KRISENSTABS

Ein kritisches Ereignis kann sich auf verschiedene Bereiche des Unternehmens auswirken und haben oft einen Einfluss auf mehrere Bereiche. Aus diesem Grund passen immer mehr Unternehmen ihre Organisationsstruktur an, um einen ganzheitlichen Ansatz im Umgang mit schwerwiegenden Vorfällen zu ermöglichen.
Die Bildung eines «Overlay-Teams», welches sich um die grösseren Vorfälle kümmert, macht durchaus Sinn. In einem solchen Team kommen Ressourcen, Fachwissen und Informationen aus den verschiedenen Bereichen zusammen. Dies mit dem alleinigen Ziel, die Fähigkeit zu steigern, um zu erkennen, zu verhindern und zu reagieren. Auf diese Weise kann ein verbesserter Umgang mit einem kritischen Ereignis erzielt werden, unabhängig von dessen Umfang.

Wenn dies jedoch nicht möglich ist, besteht die beste Vorgehensweise darin, übergreifende Allianzen aufzubauen. Personen in den Funktionen auf C-Level wie bspw. der Chief Information Security Officer (CISO), der Chief Technology Officer (CTO) oder der Chief Operating Officer (COO) gleichen ihre Erkenntnisse regelmässig ab und erhöhen damit die Fähigkeit einen passenden Umgang mit einer Bedrohung zu erreichen. Die Erfahrung, Einblicke und Informationen aus dem gesamten Unternehmen zusammenzunehmen, machen es möglich, schneller eine Reaktion auf einen Vorfall einzuleiten und so die Betriebskontinuität sicherzustellen.

3. BEWERTEN SIE IHRE RISIKEN UND QUELLEN VON INFORMATIONEN

Mit einem Plan und einem vorhandenen Krisenstab ist es an der Zeit zu beurteilen, wie gut das Unternehmen mit kritischen Ereignissen umgehen kann. Eines der grössten Probleme ist, nicht zu wissen, wann sich eine Bedrohung entwickelt und dann nicht in der Lage zu sein, zu überprüfen, was passiert ist.

Wenn Menschen Ereignisse und Risiken bewerten, greifen sie in der Regel auf eine Reihe von Informationen aus einer Vielzahl von Quellen zu. Diesen fehlt es teils an Details oder sie sind gar widersprüchlich. Ziel ist es, das Bedrohungsereignis zu bestätigen und dem Krisenstab alle benötigten Informationen an einem Ort zur Verfügung zu stellen, damit diese entsprechende Entscheidungen fällen können. Das bedeutet, vertrauenswürdige Informationsquellen auszuwählen, diese Informationen aufzubereiten und in einer geeigneten Form anzubieten.
Dieses Unterfangen kann insbesondere in grösseren Unternehmen schnell komplex werden. Der Beginn ist, zu verstehen, wo ein Ereignis im Kontext der zentralen fünf Vermögenswerte einzuordnen ist.
Diese sind: Menschen, Gebäude, IT-Systeme, Lieferkette und Marke/Reputation. In einigen Fällen können Organisationen diesen Vermögenswerten sogar einen bestimmten Wert zuordnen, um das Risiko besser bestimmen zu können.

Abb2: Suchen und bewerten von Risiken

4. IDENTIFIZIEREN SIE KRITISCHE ANLAGEN / FUNKTIONEN UND RISIKEN

Bei jedem Ereignis ist es wichtig zu wissen, wo sich Mitarbeiter, Besucher, Büros, Infrastruktur und andere kritische Vermögenswerte des Unternehmens befinden. Es ist auch wichtig zu wissen, in welcher Abhängigkeit diese zueinanderstehen.

Idealerweise können Unternehmen dies auf einen Blick visualisieren.

Häufige Beispiele für Betriebsvermögen sind:

++ Mitarbeiter
++ Produkte / Services
++ Informationen / Betriebsgeheimnisse
++ IT-Assets
++ Marke / Reputation

Neben der Kenntnis des Standortes und der Abhängigkeiten brauchen Unternehmen auch eine Vorstellung davon, wie viel es kosten wird, wenn diese Vermögenswerte von einem Ereignis betroffen sind.
Wenn beispielsweise eine kritische Geschäftsanwendung ausfällt, führt dies schnell zu einem enormen Schaden. Es ist wichtig, den Schaden basierend auf einem Anwendungsfall zu berechnen, bspw. wie viele Mitarbeiter sind davon beeinträchtigt.

Unternehmen müssen immer häufiger mehr darauf achten, dass die Marke bzw. der Ruf keinen Schaden nimmt und weniger darauf, welche materiellen Vermögenswerte davon betroffen sind. Ein «Shitstorm» von Tweets könnte weitaus mehr Schaden anrichten als ein physischer Angriff auf das Unternehmen oder seine Infrastruktur. Ebenfalls ist es gerade für Unternehmen, welche in der Datenverarbeitung tätig sind, besonders gefährlich, wenn es sich beim eingetroffenen Ereignis um eine Verletzung des Datenschutzes oder einen Cyberangriff handelt. Hier kann der Reputationsschaden im Extremfall sogar über das Fortbestehen des Unternehmens entscheiden.

Abb3: Identifikation von kritischen Vermögenswerten

Der nächste Schritt besteht darin, herauszufinden, was kritisch ist und was nicht. Die zentrale Frage hier ist - Was sind die Auswirkungen und wie gross ist das Ausmass?

Ein effektiver Ansatz besteht darin, zwischen Bedrohungen und Risiken zu unterscheiden und dann das Risiko zu quantifizieren, basierend auf folgenden Faktoren:

++ Die Bedrohung
++ Die Art der Bedrohung
++ Die allgemeine Verwundbarkeit oder Gefährdung der Unternehmung
++ Die Gesamtauswirkung, (geht möglicherweise über Vermögenswerte / Personen hinaus)

Leider ist dies keine einfache Gleichung, da Unternehmen einige weitere Faktoren berücksichtigen müssen. Es gilt die allgemeine Zeitachse zu betrachten, diese ist sehr oft dynamisch. Zum Beispiel reicht es nicht aus, zu fragen: „Wie viele Mitarbeiter arbeiten am Hauptsitz?", da die Mitarbeiter unterwegs oder sonst gerade abwesend sein können. Oder nehmen wir die Pandemie als weiteres Beispiel, dieses Ereignis hat eine Unterbrechung der Lieferkette verursacht, die Auswirkungen dessen sind aber meist erst Monate später spürbar. Da würde es also zu kurz greifen, nach Ausbruch der Pandemie festzustellen, wir sind von keinem Engpass betroffen, wenn dieser Effekt erst noch seine Auswirkung zeigen wird.

Obwohl es wichtig ist, das Risiko zu quantifizieren, müssen Sie bedenken, dass die Auswirkungen eines einzelnen Ereignisses im Unternehmen an unterschiedlichen Stellen seine Auswirkungen zeigen kann. Mit anderen Worten, der Kontext ist wichtig und dies kann das Risikoprofil ändern. Der Schlüssel ist, das Risiko basierend auf allen Variablen zu verstehen, um die beste Reaktion darauf zu ermitteln.

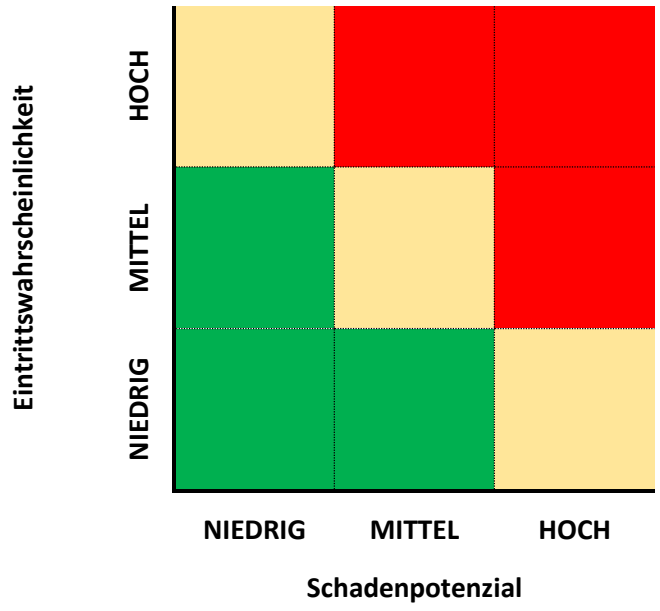

Abb4: Einfache Risiko-Matrix

5. IDENTIFIZIEREN UND FINDEN SIE ALLE STAKEHOLDER

Mitarbeiter in Krisensituationen schnell zu finden, mit ihnen zu kommunizieren und zu helfen, ist eine der obersten Prioritäten. In der Regel sind in einem Unternehmen bei kritischen Ereignissen folgende drei Interessengruppen von Wichtigkeit:

+++ Die Personen, die etwas zur Behebung des Ereignisses beitragen können. Diese Personen können die Situation in Kontext setzen und helfen, die Bedrohung besser einzuschätzen. Weiter kann diese Interessengruppe bei der Lösung helfen.

+++ Eine weitere Interessengruppe sind die direkt betroffenen. Diejenigen, die direkt von einem Ereignis betroffen sind, müssen Bescheid wissen über den weiteren Verlauf und die nächsten Schritte.

+++ Die dritte Interessengruppe ist das Management. Hier gilt es aber jeweils abzuwägen, ob ein CEO um 2 Uhr morgens geweckt werden muss, oder ob die Benachrichtigung dessen auch später noch möglich ist. Natürlich gibt es Ereignisse, welche keinen Zweifel daran lassen, dass auch ein CEO seinen Schlaf unterbrechen muss, da das Ausmass so gross ist und es unverzüglich weitreichende Entscheidungen braucht.

Um «Alarmmüdigkeit» vorzubeugen, sollte es vermieden werden, Personen unnötig zu informieren. Je öfter dies passiert, desto weniger ernst wird die Lage genommen und eventuell fälschlich auch mal als nicht kritisch erachtet.

Die involvierten Interessengruppen müssen regelmässig über den Stand informiert werden. Hier gilt es aber, mit Bedacht vorzugehen, um ein «bombardieren» mit Aktualisierungen zu vermeiden. Es ist hilfreicher, wenn die Informationen an einem zentralen Ort einsehbar sind, so kann jede Personengruppe auch selbst noch entscheiden, wie tief sie sich informieren will und erhält so das richtige Mass an Informationen. Dies heisst aber nicht, dass die regelmässigen Updates gestrichen werden können.

6. VERBESSERN SIE DAS VERSTÄNDNISS MIT EINER VISUALISIERUNG

Um das Verständnis zu verbessern ist es eine effektive Methode Informationen zu visualisieren. Dadurch wird das allgemeine Verständnis und die Informationsqualität verbessert, da die Informationen einen anderen Gehalt haben als reiner Text. Darauf basierend haben die involvierten Personen ein gleiches Bild und können besser in den Prozess Einblick nehmen, der dieses Ereignis ausgelöst hat. Wenn jeder weiss, bspw. wie viele Personen betroffen sind, welche Services oder Systeme betroffen sind, woran aktuell gearbeitet wird, dann wird dies die Zeit bis zur Entstörung verkürzen, was die Effektivität steigert.
Es ist dazu wichtig, dass die jeweiligen Personen die richtigen Informationen sehen, um sie dabei zu unterstützen, eine fundierte Entscheidung zu treffen und keine Zeit damit zu verschwenden, die Informationen zuerst deuten zu müssen.

Diese Punkte können als drei Best Practices angesehen werden:

++ Zu wissen, wann Sie die entsprechende Personengruppe sowie Funktionen mit einbeziehen
++ Zu wissen, wann Sie das Notfallszenario initiieren
++ Vorbereitet zu sein, mit mehreren Interessengruppen umzugehen und einen Workflow für komplexe Situationen bereitzuhalten

Abb5: Eine Visualisierung steigert das allgemeine Verständniss

7. ABLAUF ANALYSIEREN

Nach einem Ereignis ist vor einem Ereignis. In diesem Sinne, ist der letzte Schritt in diesem Kreislauf besonders wichtig, es soll analysiert werden, wie gut der Plan und die Abläufe funktioniert haben. Diese Debriefing nach einem Vorfall nicht durchzuführen ist eine verpasste Chance, um aus dem erlebten für die Zukunft zu lernen. Auch wenn ein Prozess noch so gut durchdacht ist und auch ausgezeichnet funktioniert hat, gibt es immer noch kleine Verbesserungsmöglichkeiten. Oder schlicht neue Erfahrungen, welche in die Entwicklung miteinfliessen sollen.

In einem solchen Debriefing sollten beispielsweise folgende Punkte Platz finden:
++ Wurde etwas Wichtiges in der Planung vergessen oder vernachlässigt?
++ Hat sich ein Effekt gezeigt, an den so noch nicht gedacht wurde?
++ Sind wichtige Interessengruppen nicht zeitgerecht informiert worden?
++ Ist so ein Ereignis schon mal passiert?
++ Welche Auswirkungen haben sich gezeigt und waren dies wie erwartet?
++ Was hat gut funktioniert?
++ Was hätte besser gemacht werden können?
++ Wurde das RTO (Recovery Time Objective) eingehalten?

Im Idealfall sind Antworten auf diese und weitere Fragen vorhanden, da diese an einem zentralen Ort abgelegt wurden. Der Schlüssel für eine noch bessere Reaktion in der Zukunft liegt darin, diese Abläufe zu überprüfen und so den KVP-Kreislauf zu schliessen.

Wird dieser Prozess mit der nötigen Sorgfalt und gewissenhaft betrieben, wird der Reifegrad des Krisenmanagements ständig besser. Dadurch wird das Unternehmen folgende Vorteile erzielen:

1. Verbesserung der operativen Effizienz und Effektivität im Umgang mit Krisen
2. Vermeidung von unnötig lange Betriebsunterbrechungen und eine verbessertes RTO, was sich positiv auf Ihre Vermögenswerte auswirkt
3. Ein Erhöhen der Widerstandsfähigkeit, indem Sie auf Risiken vorbereitet sind und diese dadurch minimieren und so die Gefahr für Mitarbeiteten und das Unternehmen im Allgemeinen senken

FAZIT

Da Unternehmen mit einer wachsenden Anzahl von Bedrohungen konfrontiert werden, sind sie gut beraten, ihre operative Reaktion darauf zu planen, durchzuspielen und sich darauf vorzubereiten.
Von Unternehmen wird erwartet, dass sie ihre Mitarbeiter und weiteren Vermögenswerte vor Bedrohungen schützen. Dazu ist es elementar, dass ein Unternehmen schnell über Informationen zu einem kritischen Ereignis verfügt und unverzüglich weiss, wie es darauf reagieren soll. Dies mit dem Fokus, die Auswirkungen für alle Beteiligten multidimensional zu reduzieren.
Mithilfe von ausgereiften Prozessen / Plänen, geschulten Mitarbeitenden und einem Krisenstab, der über die nötige Erfahrung und die nötige Portion Leadership verfügt, kann bereits sehr viel zu einem abgeschwächten Ausgang beigetragen werden.
Nicht alles muss ein Unternehmen selbst machen, holen Sie sich Hilfe/Unterstützung bei externen Firmen, die Sie gerne objektiv beraten und bei Ihrem Vorhaben helfen können. Gerade der unvoreingenommene Blick von aussen, von einer Person, die schon vielfältige Situationen gesehen hat, wird für Ihr Unternehmen sehr bereichernd sein und stark dazu beitragen, dass Ihre Massnahmen gleich vom ersten Wurf an, zuverlässiger sind, als wenn Sie das alles von Grund auf neu ausarbeiten müssten.

ÜBER DEN AUTOR

Philip Helfenberger ist Geschäftsführer und Senior Consultant bei der optimus amicus GmbH ist. Er ist in dieser Rolle verantwortlich für die Themen der Informationssicherheit, er führt Schulungen sowie Audits durch und erstellt Konzepte in seinem Themengebiet.

Philip Helfenberger hat selbst 20 Jahre Erfahrung in der Informatik und davon ist er seit über 10 Jahren vertieft im Bereich Informationssicherheit tätig. In seiner Karriere war Herr Helfenberger in unterschiedlichen Branchen tätig. Er konnte sich bei Internetprovidern, Banken, Energieversorgern und IT-Dienstleistern eine grosse Expertise aneignen. In verschiedenen Projekten mit grosser Tragweite hatte er jeweils eine Schlüsselrolle.

Um sein Wissen ständig zu erweitern und unter Beweis zu stellen, verfügt er aktuell über eine grosse Anzahl an Zertifizierungen, darunter unter anderem, CISSP, CISA, CISM, ISO27001 Lead Auditor und den CCNP Security.

Seit über 7 Jahren unterrichtet Philip Helfenberger zudem bereits an höheren Fachschulen, um sein Wissen weiterzugeben. Aus diesem Grund engagiert er sich auch in der Ausbildung von Lehrlingen zum Informatiker, wo er als Prüfungsexperte die praktische Facharbeit betreut.

Philip Helfenberger ist zudem seit mehr als 10 Jahren als Geschäftsführer einer KMU tägig. Dort ist er für den langjährigen Erfolg des Unternehmens verantwortlich. Durch dieses Wissen ist ihm absolut bewusst, was ein Unternehmen erfolgreich macht.

Quellen:

BCI Horizon Scan 2021
https://www.bsigroup.com/globalassets/localfiles/en-th/iso-22301/bci-horizon-scan-report/bci-horizon-scan-report-2021-th.pdf

ENISA Threat Landscape 2021
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021