onelogin | EBOOK

Informationen zur Erstellung

Eines Business Continuity Plans

Best Practices rund um Führung, Arbeitskräfte, Security und Technologie in Krisenzeiten

Einführung

Ein erfolgreiches Unternehmen muss in der Lage sein, den Betrieb auch unter widrigen Bedingungen aufrechtzuerhalten, sei es während einer Naturkatastrophe, einer Pandemie, einer Wirtschaftskrise oder einer ähnlich kritischen Situation, die den normalen Geschäftsablauf gefährdet. Ob es nun darum geht, sicherzustellen, dass Ihre Technologie nicht ausfällt, dass Ihre Mitarbeiter sicher von zu Hause aus arbeiten können oder dass Sie mit Ihren Kunden kommunizieren können - die Entwicklung eines Notfallplans für Ihr Unternehmen, bevor eine Katastrophe eintritt, trägt zur Risikominimierung bei. Leider entwickeln viele Unternehmen erst dann einen Kontinuitätsplan, wenn es zu spät ist - mit der Folge von Unsicherheit bei den Mitarbeitern, organisatorischem Chaos und Einnahmeverlusten.

Zwar wird ein Business-Continuity-Plan im Idealfall gar nicht gebraucht, aber im Ernstfall, wenn die Dinge doch einmal außer Kontrolle geraten, rettet er möglicherweise Ihr Unternehmen. Aktuelle globale Bedrohungen wie das neuartige Coronavirus COVID-19 verdeutlichen, wie wichtig die Kontinuitätsplanung ist.

OneLogin ist der Meinung, dass Sicherheit an erster Stelle stehen sollte. Nur so können Sie Ihren Geschäftsbetrieb im Notfall oder bei schwerwiegenden Marktveränderungen am Laufen halten. Oft fragen uns Kunden nach Best Practices in diesem Bereich. Angesichts der derzeitigen Krisensituation wegen COVID-19 haben wir Ihnen daher, einen kleinen Leitfaden erstellt, der Ihnen helfen soll, die Betriebsfähigkeit Ihres Unternehmens während einer solchen Krise zu gewährleisten.

Dieser Leitfaden widmet sich insbesondere folgenden Aspekten:

- Wie wird ein Notfallplan für ein Unternehmen entwickelt und wer sollte daran beteiligt sein
- Wie sollte der Plan Kunden und Mitarbeitern gegenüber präsentiert werden?
- Was versteht man unter Business Kontinuitätsplanung und warum ist sie so wichtig?
- Welche operativen Bereiche sind einzubeziehen?

Was ist ein Business-Continuity-Plan?

Ein Business-Continuity-Plan, also ein Plan zur Gewährleistung der Geschäftskontinuität, ist den Krisenmanagementexperten von Rock Dove Solutions zufolge „eine Abfolge von Handlungen, die Ihr Unternehmen im Falle einer unerwarteten Notlage durchführen würde“. Ein solcher Plan stellt sicher, dass Sie auf verschiedene Was-wäre-wenn-Szenarien gut vorbereitet sind. Typischerweise geht es in einem Business-Continuity-Plan um besonders schwerwiegende Ereignisse wie Naturkatastrophen, Pandemien, Wirtschaftskrisen, Datendiebstähle usw.

Mit einem sorgfältig entwickelten Plan kann Ihr Unternehmen schneller auf Störungen reagieren und Risiken für Ihre Mitarbeiter, Stakeholder, Kunden und Umsätze mindern.

> ***“Eine Abfolge von Handlungen, die Ihr Unternehmen im Falle einer unerwarteten Notlage durchführen würde”***

Bestandteile des Plans

Ein allumfassender Business-Continuity-Plan widmet sich verschiedenen Bereichen. Was genau jeweils festgelegt werden sollte, hängt stark von den Abläufen im jeweiligen Unternehmen ab. Sie könnten beispielsweise einen einzelnen Masterplan erstellen oder aber mit mehreren Plänen für unterschiedliche Szenarien arbeiten. Unabhängig davon, wie Sie an Ihre Planung herangehen, müssen Sie folgende Punkte klären:

AUSLÖSER Sie benötigen eine Auflistung der möglichen Auslöser, die Ihren Plan aktivieren.

FÜHRUNG Legen Sie spezifisch fest, wie das Führungsteam interagiert und was passiert, falls ein Teammitglied ausfällt.

RICHTLINIEN FÜR HEIMARBEIT In einer Notfallsituation müssen Ihre Mitarbeiter möglicherweise von zu Hause aus arbeiten. Hierfür sollten Sie klare Regeln vorgeben.

SICHERHEITSASPEKTE Egal, in welcher Branche Sie tätig sind: Sie benötigen angemessene Sicherheitsrichtlinien, damit Ihr Geschäftsbetrieb wie gewohnt weiterlaufen kann. Können sich Ihre Mitarbeiter über eine sichere Verbindung von zu Hause aus anmelden? Ist der VPN-Zugriff ohne Probleme möglich? Und so weiter....

TEAMS Zusätzlich zur Planung der Unternehmensführung muss auch jeder Teamleiter einen Notfallplan für sein Team erstellen. Wer fungiert als Stellvertreter? Wofür ist jedes einzelne Teammitglied verantwortlich?

NOTFALLPLÄNE VON DIENSTANBIETERN Bestimmt sind auch Sie auf die Dienste wichtiger Technologieanbieter angewiesen, die Ihren Geschäftsbetrieb ermöglichen. Daher sollten Sie jeden Anbieter um eine Kopie seiner Business-Continuity-Pläne bitten.

Beteiligung aller Stakeholder

Sobald Sie sich für die Entwicklung eines Business-Continuity-Plans entschieden haben, ist es Zeit, alle relevanten Stakeholder zu versammeln und im Detail zu klären, was in den Plan aufgenommen werden soll, wer für welche Aspekte des Plans die Verantwortung übernimmt und wie der Plan Mitarbeitern und Kunden gegenüber präsentiert werden soll. Falls Sie vor dem auslösenden Ereignis noch keinen Business-Continuity-Plan entwickelt haben, muss dies schnellstens nachgeholt werden – betonen Sie also beim Gespräch mit Stakeholdern die Dringlichkeit des Projekts. Wenngleich es abhängig von Ihren spezifischen Geschäftsanforderungen Abweichungen in der Zusammenstellung Ihrer Taskforce geben kann, empfehlen wir auf jeden Fall die Beteiligung folgender Personen:

- **CEO** Als Leiter des Unternehmens spielt Ihr CEO eine zentrale Rolle bei der Entwicklung und Genehmigung Ihres generellen Plans
- **COO** Ihr Chief Operating Officer bzw. leitender Geschäftsführer behält den Überblick über das Projekt, bringt die richtigen Teams zusammen, identifiziert Risiken in Absprache mit geschäftskritischen Technologieanbietern und gibt die allgemeine Strategie vor.
- **CMO** Ihr Chief Marketing Officer bzw. Marketingleiter kann sich um die interne und externe Kommunikation kümmern. Wann werden Mitarbeiter informiert und was wird ihnen mitgeteilt? Und wie sieht es mit den Kunden aus? Zudem sollte Ihr CMO eventuelle Kommunikationslücken bewerten, damit sichergestellt wird, dass Ihr Vertriebsteam weiterhin Leads erhält.
- **CTO/CIO** Ihr Chief Technology Officer/Chief Information Officer bzw. Leiter der Technikabteilung muss sich der Frage widmen, wie gut Ihr Unternehmen für Heimarbeit aufgestellt ist.
  Können sich Ihre Teams beispielsweise in ein VPN einwählen? Haben Sie eine Plattform wie OneLogin, die den sicheren Zugriff ermöglicht? Falls Sie in der Technologiebranche tätig sind, muss Ihr CTO zudem prüfen, welche Ressourcen ausfallen könnten.
- **CISO** Die Sicherheit darf in keinem Notfallkonzept vernachlässigt werden. Ihr Chief Information Security Officer bzw. Verantwortlicher für die Informationssicherheit sollte beurteilen können, welche Daten Risiken ausgesetzt sind und welche Vorkehrungen getroffen werden müssen.
- **CRO** Ihr Unternehmen muss sicherstellen, dass Vertriebszyklen fortgesetzt werden können und Ihre Kunden auch weiterhin zufrieden sind. Ihr Chief Revenue Officer bzw. Verantwortlicher für die Umsatzgenerierung sollte klären, ob und wie Ihre Abteilungen mit direktem Kundenkontakt Telefonate entgegennehmen, effektiv von zu Hause aus arbeiten und wichtige Konversationen fortführen können.
- **CFO** Auch bei unerwarteten Notlagen müssen Sie normalerweise die Rechnungen Ihrer Zulieferer ordnungsgemäß begleichen. Und natürlich möchte Ihr Unternehmen selbst weiterhin Umsätze generieren. Ihr Chief Financial Officer bzw. Finanzchef muss also sicherstellen, dass alles auf Kurs bleibt.
- **CPO** Mitarbeiter sind Ihre wertvollste Ressource. Ihr Chief People Officer bzw. Personalleiter sollte folglich dafür sorgen, dass es angemessene Richtlinien gibt und Ihre Mitarbeiter auf dem Laufenden gehalten werden.

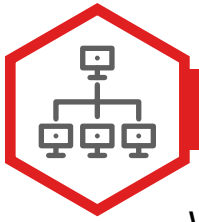
Durchführung

Einer Risikoanalyse

Wenn alle Stakeholder zusammengebracht wurden, besteht der erste Schritt auf dem Weg hin zu Ihrem Business-Continuity-Plan in der Durchführung einer Risikoanalyse. Durch eine funktionsübergreifende Risikoanalyse werden Schwachstellen innerhalb Ihres Unternehmens sowie zu klärende Probleme identifiziert. Zudem empfehlen wir, diese erfassten Risiken anhand ihrer potenziellen Auswirkungen auf das Unternehmen zu priorisieren.

Potenzielle Bedrohungen

Im Zuge der Risikoanalyse sollten Sie wichtige Risikoarten identifizieren, die unternehmensweit bestehen und denen im Notfall unbedingt entgegengewirkt werden muss. Folgende Risikoarten sind hier zu erwähnen:



MENSCHLICH

Wie wird Ihr Geschäft beeinträchtigt, wenn jemand krank wird oder gar stirbt oder wenn ein wichtiger Verantwortlicher ausfällt? Und wie gut wäre Ihr Unternehmen in der Lage, seine Geschäfte auch außerhalb der Büroräume fortzuführen, falls dies erforderlich sein sollte?

BETRIEBLICH

Wie wird der physische Betrieb in Ihrem Unternehmen durch die jeweilige Bedrohung beeinträchtigt? Welche Anlagen und Einrichtungen wären betroffen? Könnten Vertriebsprobleme entstehen?

TECHNISCH

Würde ein Ausfall von Technologien Ihre Geschäftsabläufe gefährden? Wie sieht es bei Ausfällen von geschäftskritischen Anwendungen aus oder beim Versagen der Technologie Ihrer eigenen Produkte?

FINANZIELL

Sind Sie in der Lage, weiterhin Umsätze zu generieren und Ihre Kunden zufriedenzustellen? Was wäre, wenn es an der Börse starke Schwankungen gibt oder andere finanzielle Umstände die Fortführung Ihres Geschäftsbetriebs beeinträchtigen?

SICHERHEITSTECHNISCH

Welchen physischen oder virtuellen Sicherheitsrisiken sind Sie ausgesetzt? Haben Sie geeignete Schutzvorkehrungen getroffen?

KOMMUNIKATIV

Haben Sie ein Notfallkonzept für die Kommunikation untereinander sowie mit Ihren Mitarbeitern, Kunden und anderen Stakeholdern?

Um die Vollständigkeit Ihrer Auflistung von Bedrohungen zu beurteilen, fragen Sie andere Teamleiter, welche Vorschläge sie haben und welche funktionalen Risiken sie sehen.

Sobald Sie Ihre anfängliche Liste mit potenziellen Bedrohungen aufgestellt haben, setzen Sie sich als Team an einen Tisch und besprechen Sie die Priorität jeder Risikoart und die möglichen Folgen für das Unternehmen. Hierzu empfiehlt sich die Verwendung einer Matrix, in der verschiedene mögliche Szenarien basierend auf ihrer Wahrscheinlichkeit und generellen Auswirkungen abgebildet werden.

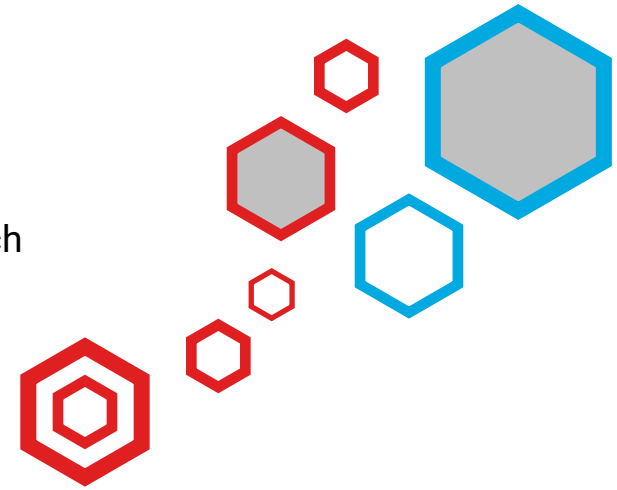
Entwicklung

Ihres Business-Continuity-Plans

In dieser Phase des Prozesses haben Sie bereits Ihr Kernteam identifiziert und diverse Risikoszenarien durchgespielt. Sie wissen inzwischen, wo Lücken auftreten und welche Fragen geklärt werden müssen. Nun wird es Zeit, Ihr konkretes Notfallkonzept zu entwickeln und festzulegen, wie Ihr Unternehmen auf Störungen reagieren soll. Ziel ist es, Ihren Plan in einem Dokument festzuhalten, das Sie sowohl intern als auch extern verteilen können, damit jeder weiß, was er im Notfall zu tun hat.

Einweisung der Mitarbeiter

Bei der Entwicklung Ihres Notfallkonzepts haben Ihre Mitarbeiter oberste Priorität. Sie müssen sicherstellen, dass Ihre Teams genau wissen, wer die Verantwortungsträger sind und wie vorzugehen ist, falls der Zugang zu den Büroräumen nicht möglich ist. Wenn Ihre Mitarbeiter unsicher sind, wie sie sich in einer Krisensituation zu verhalten haben, befindet sich Ihr Unternehmen in einer äußerst prekären Lage.



Führung und funktionale Teams

Klären Sie unbedingt, wie der Ausfall einer Führungskraft oder eines wichtigen Verantwortlichen kompensiert werden soll. Wenn beispielsweise der CEO, CMO oder CFO in Ihrem Führungsteam plötzlich arbeitsunfähig ist, muss festgelegt sein, wer als Stellvertreter fungiert. Sie benötigen also eine Richtlinie, die vorgibt, wer unternehmensweit die Führung übernimmt und ob es Leiter von funktionalen Teams gibt, die bei Bedarf auch eine temporäre Führungsposition einnehmen könnten.

Redundanz in der Führungsriege ist allerdings nicht die einzige personelle Herausforderung, die es zu bewältigen gilt. Auch für die einzelnen Teams muss definiert werden, was beim Ausfall eines wichtigen Teammitglieds passieren soll. Gibt es jemanden, der die Aufgaben des ausgefallenen Mitglieds übernehmen könnte? Falls die Beantwortung dieser Frage schwerfällt, sollte das Team seine Rollen dokumentieren und jeweils einen entsprechenden Kollegen einbeziehen, damit dieses institutionelle Wissen auf eine Gruppe verteilt wird und nicht nur bei einer Person verbleibt.

Richtlinien für Heimarbeit

Angesichts der dynamischen Arbeitswelt in unserer heutigen Zeit ist Heim- und Telearbeit nichts Ungewöhnliches. Viele Unternehmen haben jedoch keine dokumentierten Richtlinien hierfür und auch keinen Plan für den Fall, dass in einer Krisensituation jeder von zu Hause aus arbeiten müsste. Wäre das Unternehmen noch handlungsfähig?

Unter anderem sind folgende Fragen zu klären:

- Haben Sie ein virtuelles privates Netzwerk (VPN) , falls ja, können alle Mitarbeiter des Unternehmens ordnungsgemäß von außerhalb darauf zugreifen?
- Gibt es physische Netzwerkeinschränkungen für den Remotezugriff? Falls dem so ist, sollten Sie eine Strategie entwerfen, wie Ihre Teams in der Cloud anstelle der lokalen Systemumgebung arbeiten können.
- Nutzen Sie eine IAM-Lösung (Identity and Access Management), wie sie auch OneLogin anbietet, die Ihren Mitarbeitern den Zugriff auf Systeme und Daten von zu Hause aus ermöglicht, ohne dass zusätzliche Risiken und Sicherheitslücken entstehen?
- Sind Sie mit Kommunikationsmethoden wie Zoom oder anderen Tools für Webkonferenzen vertraut, die Ihnen die effektive Kommunikation erleichtern?

Sobald Sie herausgefunden haben, ob es irgendwelche Einschränkungen bei der Heim- und Telearbeit gibt, sollten Sie Ihre Erwartungen allen Mitarbeitern gegenüber klar kommunizieren, damit sie wissen, wie während der Krise interagiert wird und was von ihnen erwartet wird, solange sie von zu Hause aus arbeiten müssen.

Planung für funktionale Teams

Jeder Teamleiter sollte mit seinem Team das Vorgehen bei einer Krisensituation klären. Was passiert, wenn der Teamleiter ausfällt? Benennen Sie unbedingt einen Stellvertreter und möglichst sogar einen Stellvertreter für den Stellvertreter. Bedenken Sie außerdem, wer im Team geschäftskritische Funktionen innehat oder verwaltet. Was würde zum Beispiel passieren, wenn ein Teammitglied ausfäldas normalerweise den Zugang zu einem wichtigen System regelt? Könnte jemand anders diese Aufgabe übernehmen?

Funktionsorientierte Pläne könnten Sie wie folgt strukturieren:

Funktionale Wiederherstellungsteams

Leiter: _____

Stellvertr. Leiter 1: _____

Stellvertr. Leiter 2: _____

Teammitglieder: _____

Verantwortlichkeiten:

Erstellen Sie eine Liste mit den geschäftskritischen Vorgängen, für die Ihr Team verantwortlich ist.

Beispiele:

- Wiederherstellung der Services für Kunden
- Beaufsichtigung und technische Anleitung anderer Teams
- Technische Entscheidungen nach Bedarf
- Überwachung des allgemeinen Zustands und der Leistungsfähigkeit der Services
- Übermittlung zeitnaher Statusaktualisierungen
- Einbindung und Koordination mit wichtigen Dienstanbietern

Aufgaben:

Erstellen Sie eine Liste mit den nötigen Aufgaben Ihres Teams für den Krisenfall.

Beispiele:

- Vertrautheit mit diesem Plan sicherstellen
- Leicht abrufbare Kontaktdaten für Technologiedienstanbieter und Partner erfassen
- Leicht abrufbare Kontaktdaten für Kunden erfassen
- Backup-Kopien aller Daten, Betriebssystemabbilder, Konfigurationen, Programmcodes (Quelltext und Binärdateien) und Tools anlegen
- Checklisten für Installationen und Konfigurationen sowie Standardversionen und Betriebshandbücher erstellen
- Kommunikationsfolgen bestimmen

Krisenkommunikations

Damit Ihr Business-Continuity-Plan erfolgreich umgesetzt werden kann, benötigen Sie zwingend eine effektive Kommunikationsstrategie. Diese legt fest, wie Sie mit Ihren Mitarbeitern, Ihren Kunden und anderen betroffenen Partnern oder Zulieferern kommunizieren. Federführend bei der Entwicklung Ihrer Kommunikationsstrategie könnten Ihre Marketing- und Personalabteilung sein.

INTERNE KOMMUNIKATION

Die klare Kommunikation mit Ihren Mitarbeitern kann über den Erfolg oder Misserfolg Ihres Plans entscheiden. Stellen Sie sicher, dass alle Mitarbeiter verstehen, was vor sich geht, wie der Geschäftsbetrieb beeinträchtigt ist und was spezifisch von ihnen erwartet wird. Falls die Krisensituation Heimarbeit erfordert, informieren Sie Ihr Personal, welche Arbeitszeiten einzuhalten sind, wie die Verbindung mit dem Unternehmensnetzwerk hergestellt wird, wie miteinander kommuniziert werden soll und wie Ihre Führungsriege alle Mitarbeiter auf dem Laufenden hält. Achten Sie außerdem darauf, dass jede Führungskraft eines funktionalen Teams die Weisungshierarchie kommunizieren kann.

Während einer Krisensituation fragen sich Ihre Mitarbeiter wahrscheinlich besorgt, wie es wohl weitergehen wird. Wir empfehlen daher, sie täglich via E-Mail oder Slack oder mit Neuigkeiten direkt aus der Führungsetage auf dem Laufenden zu halten.

EXTERNE KOMMUNIKATION

Die Übermittlung von aktuellen Informationen an Kunden sollte sofort nach Aktivierung Ihres Business-Continuity-Plans beginnen. Abhängig von Ihrer Branche und dem Ausmaß der Störungen Ihres Geschäftsbetriebs genügt es möglicherweise, Ihre Kunden einfach mit einigen kurzen E-Mail-Mitteilungen über die zu erwartenden Verzögerungen und Ausfälle zu informieren. Falls Ihre Technik oder Produktionskapazität beeinträchtig ist, sollten Sie hingegen detailliertere Angaben und Zeitpläne übermitteln.

Bei besonders kritischen Situationen empfehlen wir die Nutzung mehrerer Kommunikationskanäle, z. B. Telefon, E-Mail, App-Benachrichtigungen usw. Stellen Sie zudem sicher, dass Ihre Kundenteams für Kunden direkt via Handy oder Videokonferenz erreichbar sind.

Eventuell bitten Kunden Sie auch vorsorglich um eine Kopie Ihres Business-Continuity-Plans – diese Informationen sollten Sie also stets zur Hand haben.

Dienstunterbrechungen und technische Abhängigkeiten

Wenngleich jedes Unternehmen seine technischen Schwachstellen evaluieren sollte, stellen Dienstunterbrechungen jedoch vor allem diejenigen Unternehmen vor große Herausforderungen, die Technologiedienstleistungen als ihr

Mögliche Fragen wären zum Beispiel:

- Nutzen Sie Cloud-Technologien oder sind Sie vorwiegend auf lokale Systeme angewiesen? Welches Vorgehen ist im Falle von lokalen Systemen mit erforderlichem Zugriff auf physische Server geplant, wenn Ihre Mitarbeiter von zu Hause aus arbeiten müssen? Gibt es eine einzelne Person, die Sie mit der Serverüberwachung beauftragen könnten?

- Stammen die Systeme und Dienste in Ihren Rechenzentren von verschiedenen Anbietern oder sind Sie von einem einzelnen Anbieter abhängig? Falls Sie Dienste von einem Cloud-Dienstanbieter wie AWS beziehen, werden Ihre Ressourcen wahrscheinlich über mehrere Regionen hinweg redundant bereitgestellt. Das heißt, wenn eine Region nicht mehr erreichbar ist, droht in den meisten Fällen dennoch kein Systemausfall.

- Welche Dienstanbieter sind für den unterbrechungsfreien Betrieb Ihrer Technologien nötig und kennen Sie deren Business-Continuity-Pläne? Falls nicht, bitten Sie die betreffenden Dienstanbieter um eine Kopie dieser Pläne.

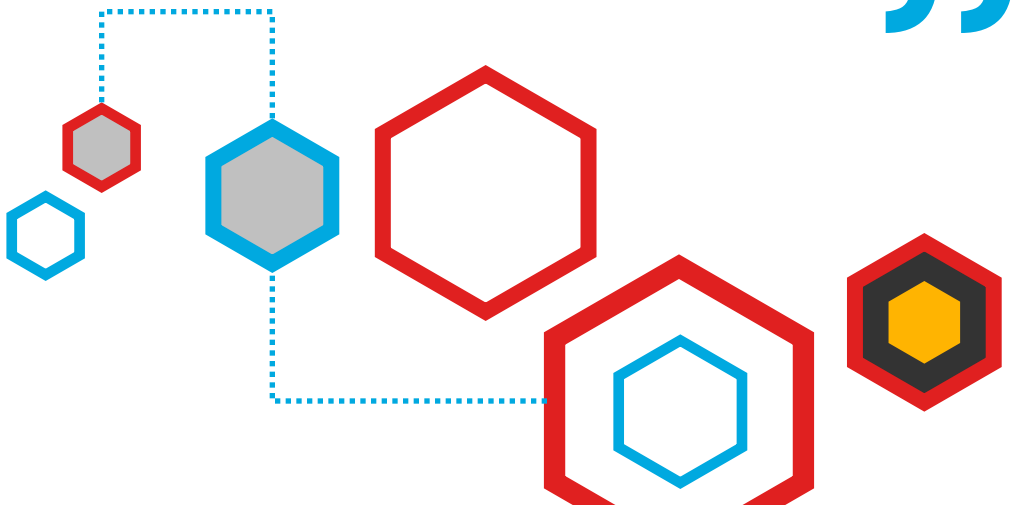
Sicherheitslücken

Ihre Sicherheitsteams sollten unbedingt potenzielle Risiken und Datenschutzlücken in verschiedenen Krisensituationen eruieren. Wenn Ihre Mitarbeiter zum Beispiel längere Zeit von zu Hause aus arbeiten müssen, brauchen Sie eine Lösung für die ordentliche Identitäts- und Zugriffsverwaltung, beispielsweise das IAM-Tool von OneLogin, damit sämtliche Anmeldeversuche kontrolliert werden können. Heimarbeitssysteme sind ein beliebtes Ziel für Hacker – seien Sie also auf der Hut und sorgen Sie für angemessenen Schutz.

Denken Sie auch daran, Ihre Mitarbeiter über alle potenziellen Sicherheitslücken zu informieren. Je nachdem, um was für eine Art Krise es sich handelt, befinden sich womöglich schon so manche Gauner und Trickbetrüger in Lauerstellung, um die Ängste der Bevölkerung auszunutzen. OneLogin erfuhr schon fast unmittelbar nach dem Ausbruch der Coronavirus-Pandemie von den ersten Phishing-Angriffen, mit denen sich Cyberkriminelle die Sorgen und das Informationsbedürfnis der Menschen zunutze machen wollten, um Passwörter, Daten und andere Habseligkeiten zu entwenden. Beispielsweise wurden E-Mails mit gefälschter Absenderadresse versendet, die es so aussehen ließen, als ob die Nachrichten von der Weltgesundheitsorganisation (WHO) stammten. Die Empfänger wurden dann um Spenden an betrügerische Wohltätigkeitseinrichtungen gebeten oder sollten auf einen Link in der E-Mail klicken, wodurch heimlich Schadsoftware auf ihre Rechner gelangt wäre.

Wenn Ihre Mitarbeiter von zu Hause aus arbeiten, sind sie anfälliger für Phishing und andere Betrugsarten. Eine IAM-Plattform mit Multi-Faktor-Authentifizierung zum Schutz Ihres Unternehmens vor Datenlecks ist heutzutage quasi unverzichtbar.

> ***Je nachdem, um was für eine Art Krise es sich handelt, befinden sich womöglich schon so manche Gauner und Trickbetrüger in Lauerstellung, um die Ängste der Bevölkerung auszunutzen***



Reaktionsphasen und beispielhafte Abläufe

Nachdem Sie Ihren Business-Continuity-Plan verfasst haben, müssen Sie festlegen, welche Aktionen in welcher Reihenfolge Schritt für Schritt durchzuführen sind. Die in diesem Abschnitt erwähnten Abläufe sind bewusst sehr allgemein gehalten. Jede Krisensituation ist einzigartig und

PHASE I Erkennung einer möglichen Katastrophe

Wer sollte das tun?	Was ist zu tun? Wann?
Alle Unternehmensmitglieder	Achten Sie ständig auf Situationen und Ereignisse, die katastrophale Folgen haben könnten.
Person, die einen Störfall bemerkt	⬢ Prüfen Sie, ob Menschen in Gefahr sind und welche Sicherheitslücken entstehen. Informieren Sie sofort den örtlichen Rettungsdienst (Feuerwehr, Notarzt, Polizei). ⬢ Prüfen Sie, ob Unternehmenseigentum in Gefahr ist. ⬢ Informieren Sie möglichst zeitnah eine Führungskraft (Abteilungsleiter oder höher).
Leitender Angestellter, der auf den Zwischenfall reagiert	Informieren Sie sofort die Teammitglieder.

PHASE II Ausrufung des Katastrophenfalls

Wer sollte das tun?

Führungsstab

Was ist zu tun? Wann?

- Sammeln Sie Fakten. Holen Sie unterstützende Berichte oder Beweise ein.
- Rufen Sie den Katastrophenfall aus. Aktivieren Sie den plan.
- Weisen Sie eine Führungskraft an, die Teams für die Notfallwiederherstellung zu benachrichtigen und zu versammeln.
- Informieren Sie Ihr Krisenkommunikationsteam.
- Legen Sie einen Zeitplan und eine Methode für die weitere Kommunikation fest (z. B. „in einer Stunde per Konferenzschaltung über eine bestimmte Einwahlnummer“).

PHASE III Mobilisierung

Wer sollte das tun?	Was ist zu tun? Wann?
Einsatzleiter (oder Vertreter)	● IInformieren Sie alle Teamleiter mittels Anrufbaum oder vergleichbarem Verfahren, dass ein Katastrophenfall eingetreten ist und der Plan aktiviert wurde. ● Erinnern Sie die Teamleiter an diesen Plan und weitere hilfreiche Ressourcen und unterstützen Sie sie beim Zugriff auf nötige Informationen.
Teamleiter	● Informieren Sie sofort die Teammitglieder. ● Trommeln Sie das Team zusammen. ● Weisen Sie Aufgaben zu, um die Art, das Ausmaß und den Ort des Schadens zu bestimmen. ● Entscheiden Sie sich für eine Methode zur Kommunikation und Koordination in Echtzeit und informieren Sie Ihre Teammitglieder diesbezüglich. Die Teammitglieder sollten bis auf Weiteres quasi permanent in Kontakt stehen. Die Teamleiter können entscheiden, ab
Führungsstab	● Bleiben Sie in Kontakt mit den Teammitgliedern, leiten Sie sie und erhalten Sie zeitnahe Statusaktualisierungen. ● Informieren Sie sofort die Teammitglieder.

PHASE IV Veranstaltungsmanagement

Wer sollte das tun?	Was ist zu tun? Wann?
Führungsstab	• Fragen Sie alle Teams in vernünftigen zeitlichen Abständen nach den durchgeführten Aktionen und dem Wiederherstellungsstatus. • Treffen Sie nach Bedarf strategische Entscheidungen, um die Teams und alle anderen Unternehmensangehörigen anzuleiten. Legen Sie Prioritäten, Richtlinien und Grenzen fest. Stellen den Teams benötigte Ressourcen bereit. • Entscheiden Sie, ob der Notfall finanzielle Mittel erfordert und in welcher Höhe (z. B. für Ersatzausrüstung). • IBeziehen Sie geschäftskritische Dienstanbieter ein. • Sorgen Sie für die Planung, Prüfung, Bearbeitung und Freigabe von Mitteilungen an außenstehende Stakeholder (Kunden, Vorstand, Behörden, Presse) durch das Krisenkommunikationsteam. • Der CEO, COO, CFO oder Technikleiter sollte bei Bedarf persönlich mit den Behörden kommunizieren, beispielsweise mit der Polizei oder Aufsichtsbehörden. • Legen Sie fest, was bis zur vollständigen Klärung des Katastrophenfalls noch geschehen soll, zum Beispiel wann und wie weitere interne Aktualisierungen übermittelt werden.
Krisenkommunikationsteam	• Geben Sie Texte zur Benachrichtigung externer Stakeholder (Kunden, Presse) und des Vertriebs frei. • Kümmern Sie sich um die Kommunikation und Erwartungen wichtiger Stakeholder.

Testen des Plans

Ihren Plan sollten Sie mindestens einmal im Jahr auf die Probe stellen. Die Verantwortung hierfür trägt Ihr Sicherheitsteam. Durch diesen Test können Sie potenzielle Lücken schnell identifizieren und Ihren Plan gegebenenfalls anpassen. In diesem Abschnitt stellen wir Ihnen verschiedene Testoptionen vor.

Benachrichtigungstest

Ein Benachrichtigungstest sollte mindestens halbjährlich stattfinden. Folgende Schritte sind Teil eines solchen Tests:

1. Der Testleiter kontaktiert alle Personen auf der Notfallkontaktliste über die zuvor festgelegten Kommunikationskanäle (z. B. per Handy, E-Mail, SMS oder durch persönlichen Kontakt). Dabei sollte aus der Nachricht hervorgehen, dass es sich nur um einen Kommunikationstest handelt und nicht um einen echten Notfall.
2. Der Testleiter protokolliert, wie viel Zeit zwischen der ersten Kontaktaufnahme und der Bestätigung der jeweiligen Person vergeht.
3. Nach einer vorab definierten Zeitspanne (z. B. nach 1, 2 oder 4 Stunden) wird der Test abgeschlossen und alle Personen, die nicht rechtzeitig reagiert haben, werden als Kommunikationsfehler gewertet.

Ein solcher Test kann bei Bedarf im Voraus angekündigt werden (dies wäre jedoch weniger realistisch). Da nur etwa 24 % der Stunden eines Jahres reguläre Arbeitsstunden sind, sollte überlegt werden, diesen Test auch nachts, an Wochenenden oder an Feiertagen durchzuführen.

Die Ergebnisse des Tests werden am besten in einem kurzen Memo an den CISO dokumentiert, und zwar zusammen mit wichtigen Statistiken (Anteil erfolgreicher Kontaktversuche sowie kürzeste, mittlere und längste Reaktionszeit), Angaben zu eventuell nicht vertretenen Kompetenzbereichen und eventuellen Verbesserungsempfehlungen.

In Vorbereitung auf den Test und nach Auswertung der Ergebnisse können Sie nötige Anpassungen an Ihrem Business-Continuity-Plan vornehmen.

Table-Top Test

Ein Tabletop-Test ist eine Simulation eines Katastrophenfalls oder anderen Störfalls, die in Form einer konferenzartigen Besprechung durchgespielt wird. Tabletop-Tests zeichnen sich üblicherweise durch folgende Merkmale aus:

1. Der Test wird von einem Fachexperten geplant, durchgeführt und koordiniert.
2. Der geplante Test besteht aus einem spezifischen Störfall und einem oder mehreren späteren Ereignissen (Entwicklungen) im selben Szenario. (Ein denkbares Szenario wäre zum Beispiel die Nichterreichbarkeit einer „Availability Zone“ Ihres Cloud-Dienstanbieters aufgrund eines totalen Stromausfalls.)
3. Mit den Mitgliedern Ihres Führungsteams und anderen wichtigen Verantwortlichen für Ihre Business-Continuity-Planung wird vorab ein Termin für den Test vereinbart. Über das Szenario werden sie jedoch erst zu Beginn des Tests informiert.
4. Die Teilnehmer werden durch den Testleiter einbezogen, zum Beispiel durch Fragen wie „Was würden Sie tun?“.
5. Der Testleiter protokolliert die Simulation.
6. Nach dem Test erstellt der Testleiter einen Bericht mit generellen Schlussfolgerungen und Verbesserungsempfehlungen.

Wenngleich ein Tabletop-Test die nötigen Technologien und Prozesse zur Notfallwiederherstellung nicht praktisch auf die Probe stellt, hat er mehrere Vorteile:

1. Er ist nicht teuer. Zur Durchführung müssen die Beteiligten nur wenige Stunden ihrer Zeit aufbringen und es entstehen ihnen keine finanziellen Kosten.
2. Wichtige Teammitglieder können sich mit Ihrem Business-Continuity-Plan vertraut machen und die Wichtigkeit eines gut durchdachten Notfallkonzepts wird verdeutlicht.
3. Eine solche Übung im Team offenbart eventuelle Lücken in Ihrer Planung.
4. IDas Team übt die Zusammenarbeit unter Stress. Im Ernstfall kommt somit weniger Panik auf und die Beteiligten sind zuversichtlicher, dass sie die Lage bewältigen können, getreu dem Motto: „Wir kennen das schon und wir wissen, was zu tun ist und dass wir uns aufeinander verlassen können“.

Verwaltung des Plans

Ihr Business-Continuity-Plan sollte mindestens jährlich geprüft und aktualisiert werden. Die Verantwortung hierfür trägt wieder Ihr Sicherheitsteam. Bei der Prüfung sollten die Empfehlungen aus den Testberichten beachtet werden sowie jegliche Meldungen zu Störfällen und die als Folge vorgenommenen Verbesserungen. Das jeweilige Datum und eine Zusammenfassung der Änderungen sind in einem Versionsverlauf festzuhalten.

> ***Ihr Unternehmen muss auf Krisen und Notfälle vorbereitet sein...***

Fazit

Ihr Unternehmen muss auf Krisen und Notfälle vorbereitet sein. Indem Sie frühzeitig einen Business-Continuity-Plan erstellen, können Sie schneller reagieren, wenn tatsächlich der Ernstfall eintritt. Mit einem sorgfältig durchdachten und getesteten Plan stellen Sie sicher, dass Ihre Mitarbeiter ihre Aufgaben kennen und auch Ihre Kunden nicht im Dunkeln tappen.


onelogin