Acronis

WHITEPAPER

Geschäftskontinuität: Übergang von passiver Planung zu aktiver Risikominderung und Resilienz-Wahrung

Kleine und mittlere Unternehmen (KMUs) sind ebenso häufig Ziel von Cyberkriminellen wie Großunternehmen. Es stellt sich nicht mehr die Frage, ob ein Unternehmen angegriffen wird, sondern nur noch, wann es zur Zielscheibe wird. Unternehmen können sich auf mehrere Eventualitäten vorbereiten, indem sie auch andere Störungsszenarien aus dieser Perspektive betrachten. Störungen können das Unternehmen direkt oder seine externen Service Provider betreffen.

Ransomware-Angriff auf Kaseya

Kaseya ist ein Managed Service Provider (MSP) mit weltweiten Niederlassungen, der IT-Abteilungen und anderen MSPs eine direkte Kombilösung für IT-Management und -Sicherheit anbietet. Kaseya automatisiert das IT-Management für kleine und mittlere Unternehmen weltweit.

2021 wurden die Systeme von Kaseya zum Ziel von Ransomware. Die Cyberkriminellen verschafften sich über eine Zero-Day-Schwachstelle in der VSA-Weboberfläche des Unternehmens Zugang und konnten so die Sicherheitskontrollen beim Login umgehen. Die Ransomware wurde dann über ein gefälschtes Update im automatischen Software-Update-Tool des Systems eingeschleust.

Berichten zufolge waren 800 bis 1.500 Unternehmen, darunter 50 Direktkunden, entweder von Service-unterbrechungen oder von der Ransomware selbst betroffen. Da Kaseya eine Lösung für MSPs im IT-Bereich anbietet, wird geschätzt, dass auch Tausende von Unternehmen betroffen waren, die keine direkte Kundenbeziehung zu Kaseya hatten.

Von diesem Ransomware-Angriff waren vor allem KMUs betroffen, darunter:

- Zahnarztpraxen
- Buchhalter:innen
- Supermärkte (800 Geschäfte in Schweden mussten wegen defekter Kassen schließen)
- Schulen und Kindergärten

Ransomware hat kleine Unternehmen im Visier

Bei einem anderen Vorfall wurden schätzungsweise 240.000 NAS-Geräte (Network Attached Storage) von QNAP mit Ransomware verschlüsselt. Die Cyberkriminellen nutzten Brute-Force-Angriffe auf Anmeldedaten und machten sich bekannte Schwachstellen von QNAP zunutze, um in die betreffenden Netzwerke einzudringen. Ziel der Angriffe waren vor allem kleine Unternehmen und Homeoffices.

Cybersicherheitsforschende gehen davon aus, dass diese Serie von Angriffen auf kleine Unternehmen als „Probeläufe“ für Angriffe auf größere Unternehmen gedacht waren.

KMUs verlassen sich immer mehr auf Technologie. Sie stehen vor vielen der gleichen Herausforderungen wie Großunternehmen, wenn es um Risikoplanung und Sicherheitsmanagement geht.

Was ist ein Business Continuity-Plan?

Ein Business Continuity-Plan (BCP) ist ein Verfahren, das die Aufrechterhaltung des Geschäftsbetriebs während einer größeren Störung sicherstellt. Der erste Schritt bei der Entwicklung eines Business Continuity-Plans ist die Identifizierung der entsprechenden Assets, gefolgt von der Entwicklung eines klaren Plans zu deren Schutz.

Ein Business Continuity-Plan ist mehr als nur ein Dokument mit detaillierten Informationen – er enthält auch spezifische Anweisungen, Richtlinien und Verfahren zur Aufrechterhaltung von Systemen und Betriebsabläufen. Geschäftskontinuität sieht für jedes Unternehmen anders aus, aber der Planungsprozess selbst ist ähnlich.

Alle Business Continuity-Pläne enthalten einige gemeinsame Elemente.

Wichtige Geschäftsbereiche identifizieren

Es ist wichtig, dass Sie eine klare Vorstellung davon haben, was Sie schützen wollen. Der erste Schritt bei der Entwicklung eines Business Continuity-Plans besteht darin, die Bereiche zu identifizieren, die für Ihre Geschäftstätigkeit von zentraler Bedeutung sind. Dazu gehören die wichtigsten Geschäftsprozesse oder -funktionen.

Kritische Elemente priorisieren

Kritische und zeitkritische Prozesse und Funktionen sollten zuerst behandelt werden. Dazu gehören Kernfunktionen und umsatzgenerierende Aktivitäten sowie das Identitäts- und Zugriffsmanagement.

Gegenseitige Abhängigkeiten identifizieren

Gegenseitige Abhängigkeiten zwischen Geschäftsbereichen und -funktionen können Wiederherstellungs- und Recovery-Bemühungen erschweren. Identifizieren Sie diese im Vorfeld, um zu verstehen, wie sie zusammenarbeiten.

Tolerierbare Ausfallzeit bestimmen

Je nach Art der Krise kann der Ausfall mancher Funktionen kostspieliger sein als der Ausfall anderer Funktionen. Bei Funktionen, die finanziellen und rechtlichen Verpflichtungen unterliegen, wird eine kürzere tolerierbare Ausfallzeit angesetzt.

Die tolerierbare Ausfallzeit ist die längste Zeit, die ein Unternehmen den Ausfall einer Funktion tolerieren kann, bevor es zu irreversiblen Schäden für das Unternehmen und seinen Ruf kommt. Ausfallzeiten sind nie willkommen, aber es ist wichtig, für diese Szenarien im Voraus zu planen.

Recovery-Daten ermitteln

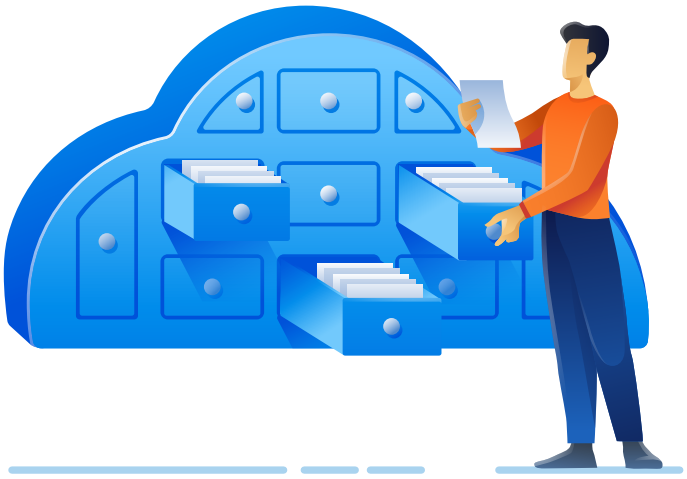
Nachdem die tolerierbare Ausfallzeit bestimmt wurde, muss sorgfältig überlegt werden, was wiederhergestellt werden soll und wie schnell dies geschehen soll. Dabei sollte neben saisonalen Geschäftszyklen, Wochentagen und Tageszeiten auch berücksichtigt werden, wie sich Betriebsstörungen auf Geschäftsabläufe, Kund:innen und Mitarbeiter:innen auswirken könnten. Die Wichtigkeit jeder Funktion bestimmt ihre Priorität bei der Wiederherstellung:

- Bestimmen Sie die kürzeste Zeit, die eine Funktion ausfallen darf, bevor langfristige Schäden entstehen.
- Funktionen mit niedriger Priorität können schnell zu Funktionen mit hoher Priorität werden, wenn sie nicht berücksichtigt werden.
- Ermitteln und überprüfen Sie für jede Funktion realisierbare Wiederherstellungsstrategien.
- Können Funktionen ausgelagert oder an einem anderen Ort ausgeführt werden? Wie lange kann diese Strategie aufrechterhalten werden?
- Können Mitarbeiter:innen von einem anderen Standort aus arbeiten (z. B. per Remote-Zugriff), wenn ihr Hauptarbeitsplatz betroffen ist?

Arbeiten Sie eng mit den wichtigsten Mitarbeiter:innen und Interessengruppen zusammen, um die Funktionen, Systeme und Daten zu identifizieren, die für die Wiederherstellung am wichtigsten sind.

Plan dokumentieren

Ein Business Continuity-Plan muss sorgfältig dokumentiert werden.
Ein nicht dokumentierter Plan hängt von den institutionellen Kenntnissen der Mitarbeiter:innen ab, die zu diesem Zeitpunkt im Unternehmen beschäftigt sind.
Die Dokumentation stellt sicher, dass der Plan auch nach einem Personalwechsel anwendbar bleibt.



Was ist eine Risikobewertung?

Unter einer Risikobewertung versteht man einen Prozess, bei dem alle Aspekte der potenziellen Risiken für die Betriebsabläufe in einem Unternehmen ermittelt und bewertet werden. Durch diesen Prozess werden potenzielle Schwachstellen aufgedeckt, bevor es zu einem Schadensfall kommt. Die Risikobewertung hilft Ihnen, sich auf Worst-Case-Szenarien vorzubereiten und dabei stabile Geschäftsabläufe zu gewährleisten, damit Ihr Unternehmen auch dann weiter bestehen kann.

Durchführung einer Risikobewertung

Unternehmen jeder Größe sollten eine Risikobewertung durchführen. KMUs sind sich möglicherweise nicht bewusst, dass sie vielen der gleichen Risiken ausgesetzt sind wie große Unternehmen. Der Verizon 2023 Data Breach Investigations Report zeigt, dass kleine Unternehmen 41 % mehr Datenschutzverletzungen erleiden als große Unternehmen und dass 68 % dieser Verstöße zu einem bestätigten Datendiebstahl führten.

Auswirkungen und Wahrscheinlichkeit von Bedrohungen bewerten

Eine Risikobewertung beginnt damit, die Auswirkungen und die Wahrscheinlichkeit potenzieller Gefahren bzw. Bedrohungen für Assets richtig einzuschätzen. Zu diesen Gefahren zählen Naturkatastrophen, Cyberbedrohungen, Pandemien und Brände. Zu den Assets gehören Menschen, betriebliche Abläufe, (geistiges) Eigentum, Gerätschaften sowie finanzielle oder vertragliche Verpflichtungen. Die Risikobewertung konzentriert sich dabei auf die möglichen Auswirkungen dieser Gefahren und Bedrohungen auf die betreffenden Assets.

Risikoanalyse: Risiken auf Assets und Standorte anwenden

Der Prozess der Risikoanalyse erfordert eine detaillierte Analyse potenzieller negativer Ereignisse, ihrer Folgen und ihrer Eintrittswahrscheinlichkeit. Sie befasst sich mit detaillierten Szenarien und Kontrollfaktoren, um deren potenzielle Wirksamkeit gegen Risiken zu bewerten, die die Assets und Standorte des Unternehmens betreffen könnten.

Risikominderung

Die Planung der Risikominderung ist ein iterativer Prozess. Wie ein Unternehmen die Risikominderung angeht, hängt von den Kundenbedürfnissen und dem Schweregrad des Risikos selbst ab. Bei der Planung der Risikominderung geht es darum, Möglichkeiten zur Verringerung von Bedrohungen aufzuzeigen.

Die Ansätze zur Risikominderung umfassen:

- Akzeptieren des Risikos: Erkennen und Akzeptieren des Risikos, ohne Maßnahmen zu seiner Kontrolle zu ergreifen.
- Vermeiden: Es werden Maßnahmen festgelegt, um das Risiko zu beseitigen oder zu verringern. Ziel ist die Vermeidung des Risikos.
- Kontrollieren: Das Risiko wird kontrolliert, um die Auswirkungen oder die Eintrittswahrscheinlichkeit des Ereignisses zu minimieren.
- Übertragen: Das Übertragen von Rechenschaftspflichten, Verantwortlichkeiten und Befugnissen auf sonstige Beteiligte oder verfügbare Drittanbieter.
- Überwachen: Das Überwachen von Risikofaktoren auf mögliche Veränderungen, die die Art oder Auswirkungen der Risiken beeinflussen könnten.

Als Teil Ihrer Risikominderungsstrategie sollten Sie die folgenden Punkte berücksichtigen:

- Machen Sie sich ein Bild von den Benutzer:innen und ihren Bedürfnissen während eines unvorhergesehenen Störereignisses.
- Konsultieren Sie Expert:innen und nutzen Sie deren Fachwissen.
- Akzeptieren Sie, dass es wiederkehrende Risiken gibt.
- Erkennen Sie, dass nicht alle Risiken gemindert werden müssen.

Kostenbewertung

Bewerten Sie die Kosten für die Risikominderung im Vergleich zu den Folgekosten für einen Schaden. Machen Sie sich ein Bild von den möglichen Kosten, bevor es zu einer größeren Betriebsstörung kommt. Identifizieren Sie geeignete Methoden zur Risikominderung und ermitteln Sie Kosten und Nutzen ihrer Umsetzung.

Entwicklung eines Plans

Entwickeln Sie einen Aktionsplan auf der Grundlage der in der Risikobewertungsphase gesammelten Informationen. Verwenden Sie die folgenden Schritte, um eine klare Struktur zu schaffen:

- Identifizieren Sie die wichtigsten Interessengruppen.
- Entwickeln Sie eine Kommunikationsstrategie für interne und externe Zielgruppen (Personal, Kund:innen, Öffentlichkeit).
- Legen Sie Teams fest, die im Ernstfall für bestimmte Aspekte des Plans verantwortlich sind.
- Ermitteln Sie die Speicherorte für System-Backups und -Wiederherstellungen und deren Funktionalität.
- Weisen Sie bestimmten Abteilungen/Geschäftsbereichen die entsprechenden Maßnahmen und Verantwortlichkeiten zu.

Warum eine herkömmliche Planung und Bewertung nicht mehr zeitgemäß ist

Herkömmliche Planungsmethoden zur Geschäftskontinuität und Risikobewertung reichen nicht mehr aus, um modernen Geschäftsanforderungen gerecht zu werden, da sie die sich ständig verändernde Bedrohungslandschaft nicht berücksichtigen. Dies kann zu ungenauen Szenarien für Recovery-Strategien führen, da sie das gleichzeitige Management mehrerer Störungen nicht berücksichtigen. So hat beispielsweise die COVID-19-Pandemie gezeigt, wie schnell Reaktionspläne durch gleichzeitig auftretende Krisen außer Kraft gesetzt werden können. Veränderungen auf den Märkten und in den Arbeitsabläufen in Kombination mit einer anhaltenden weltweiten Pandemie haben die Art und Weise, wie wir Geschäfte machen, völlig auf den Kopf gestellt.

Dauer von Ereignissen und Probleme

Die Planung kann mehrere Störfallszenarien umfassen, wobei der Schwerpunkt auf begrenzten oder lokalisierten Störungen von kurzer Dauer liegt. Der Planungsprozess basiert auf einem spezifischen Rahmen, anstatt sich auf unterschiedliche Ergebnisse zu konzentrieren. Die Planung ist isoliert und konzentriert sich möglicherweise nur auf einen bestimmten Geschäftsbereich, ohne den Rest des Unternehmens zu berücksichtigen. Die Art und Weise, wie einzelne Assets zusammenwirken, wird dabei häufig ignoriert.

Mehrere Anbieter gestört

Mehrere Anbieter können betroffen sein, was einen Dominoeffekt zur Folge hat. Drittanbieter können mit einer Vielzahl von Problemen konfrontiert sein, die sich später auf die Kund:innen auswirken können:

- Unzureichende Nachverfolgung und mangelhaftes Risikomanagement
- Mangelnde Transparenz bei gegenseitigen Abhängigkeiten zwischen Drittanbietern
- Eng fokussierte Disaster Recovery- und Business Continuity-Pläne
- Eine fehlende strategische Vision bei der Auslagerung kritischer Kompetenzen und Funktionen.

Bei der traditionellen Risikobewertung werden langfristige Betriebsstörungen nicht berücksichtigt. Da viele moderne Geschäftsprozesse miteinander vernetzt sind, können KMUs mit großen Unternehmen zusammenarbeiten. Ein scheinbar weit entferntes Ereignis kann mehrere Anbieter auf unterschiedliche Weise betreffen und zu einer Unterbrechung der Geschäftstätigkeit von KMUs führen.

Mangel an Mitarbeiterschulungen

Traditionelle Risikobewertungen berücksichtigen nicht die tatsächlichen Auswirkungen von Insider-Bedrohungen. Cyberbedrohungen entwickeln sich ständig weiter und es besteht ein ständiger Bedarf an Schulungen. Dennoch bieten viele Unternehmen keine Cybersicherheitsschulungen an, um aktuellen und neuen Bedrohungen zu begegnen.

Mitarbeiter:innen – auch diejenigen, die ein gewisses Verständnis für Cyberrisiken haben – verhalten sich möglicherweise sicherheitsgefährdend am Computer.

Viele Mitarbeiter:innen wissen nicht, dass die Cyberbedrohungen heutzutage immer ausgefeilter werden. Ihnen fehlt häufig auch das Wissen, um diese zu erkennen. In vielen Unternehmen klaffen große Lücken zwischen Wissen und Risikobewusstsein. Mitarbeiter:innen, die ein- oder zweimal im Jahr eine Cybersicherheitsschulung absolvieren, sind kaum in der Lage, potenzielle Cyberrisiken zu erkennen. Selbst grundlegende Cybersicherheitsschulungen sind selten. Cyberbedrohungen nehmen ständig zu und KMUs verfügen möglicherweise nicht über ein offizielles Schulungsprogramm oder das Budget, um ein solches zu unterstützen.

Zu viele einzelne Fehlerpunkte

Ein einzelner Fehlerpunkt ist eine Person, ein Gerät, eine Applikation oder eine andere Ressource ohne Redundanz. Einzelne Fehlerpunkte können Netzwerkgeräte oder Server, hochspezialisierte Geräte und Mitarbeiter:innen mit Spezialwissen sein, die allein die für eine bestimmte Funktion erforderliche Arbeit erledigen.

Ein Unternehmen mit mehreren einzelnen Fehlerpunkten ist anfälliger für die Auswirkungen eines ungeplanten Ausfalls oder eines Angriffs. Zu den personellen Risiken zählt der mangelnde Wissenstransfer, wenn ein Teammitglied das Unternehmen verlässt oder einen längeren Urlaub antritt – kein anderes Teammitglied kann dann die Arbeit übernehmen. Und auch der Ausfall von Spezialgeräten kann zu längeren Störungen führen. Veraltete Netzwerk- oder Servergeräte können zu Datenverlusten führen und Sicherheitsprobleme verschärfen, insbesondere wenn sie über den Service- und Support-Lebenszyklus der Geräte hinaus betrieben werden.

Eine KPMG-Studie aus dem Jahr 2020 hat zahlreiche Schwachstellen in den traditionellen Planungsmethoden für die Geschäftskontinuität aufgezeigt, wenn mehrere Ereignisse gleichzeitig eintreten, z. B. eine Pandemie, Veränderungen in der Arbeitsumgebung und -ausstattung sowie größere Marktverschiebungen. Die Ergebnisse enthielten überzeugende Daten zu massiven Veränderungen, die alle gleichzeitig auftraten und in den bestehenden Business Continuity-Plänen keine Berücksichtigung fanden.

Moderne Cyberbedrohungen: Tools zur Prävention, Erkennung, Reaktion und Wiederherstellung

Bei der Vorbereitung ist es wichtig, alle Aspekte bezüglich Prävention, Erkennung, Reaktion und Wiederherstellung kritisch zu betrachten. Die heutigen Bedrohungen für den Systembetrieb sehen etwas anders aus. Es können und werden mehrere Katastrophen gleichzeitig auftreten.

Das Auftreten einer globalen Pandemie in Verbindung mit wirtschaftlichen Turbulenzen, Lieferkettenproblemen, Naturkatastrophen (die durch den Klimawandel noch verstärkt werden) und ständig wachsenden Cyberbedrohungen, bei denen künstliche Intelligenz als Kraft-Multiplikator eingesetzt wird, hat uns in den letzten Jahren die neue Realität zusammenwirkender Bedrohungen deutlich vor Augen geführt. Anbieter sind nun in der Lage, bessere Analysen für die Vorbereitung und Bewältigung mehrerer gleichzeitiger Katastrophen bereitzustellen.

Telearbeit schafft eine neue Realität

Telearbeit hat die Unternehmen dazu gezwungen, die Netzwerksicherheit und alle neuen Geräte, die mit internen Ressourcen verbunden sind, neu zu überdenken. Dauerhafte Telearbeit erfordert einen neuen Sicherheitsansatz, denn nicht alle Geräte gehören dem Unternehmen und werden von ihm verwaltet. Der Einsatz von privaten Geräten für diesen Zweck bringt aber auch zusätzliche Sicherheitsrisiken mit sich. Mitarbeiter:innen verbinden sich von zu Hause aus und sind selbst für die Wartung und Sicherheit ihres Heimnetzwerks verantwortlich. Die Sicherheit wird zu einem noch größeren Problem, wenn Mitarbeiter:innen auf interne Ressourcen über Netzwerke zugreifen können, die sie nicht selbst verwalten.

Weniger Ad-hoc-Planung durch bessere Szenarienbewertung

Ein proaktiver Ansatz bei der Szenarienbewertung bedeutet weniger Ad-hoc-Planung, da potenzielle Störfallszenarien (soweit möglich) vor ihrem Eintreten antizipiert werden. Berücksichtigen Sie typische Gefahren und Risiken, die mit Cybervorfällen und Datenschutzverletzungen verbunden sind, sowie deren Potenzial, den Ruf der betroffenen Marke zu schädigen.

Proaktive Unternehmen können sich stärker auf Wiederherstellungsstrategien konzentrieren.

Weniger manuelle Schritte bei der Bewältigung unvorhergesehener Bedrohungen

In großen Unternehmen kann ein umfassendes Risikomanagement mit künstlicher Intelligenz und Automatisierung kombiniert werden, wodurch weniger manuelle Schritte erforderlich sind und eine schnellere Reaktion und Wiederherstellung ermöglicht wird. Je nach Art des Ausfalls oder der Katastrophe kann es jedoch eine Herausforderung darstellen, einige komplexe Aufgaben nicht mehr von Menschen ausführen zu lassen.

Bessere Vorbereitung und einfachere Schulungen

Für Recovery-Tasks werden weniger Ressourcen benötigt. Mitarbeiter:innen benötigen weniger Schulungen, um die Tools zu verwenden, und sie müssen auch nicht länger mehrere Recovery-Tasks manuell verwalten.

Pläne und Ergebnisse proaktiv überprüfen

Einen Plan zu entwickeln, nur um ihn dann in der Schublade verschwinden zu lassen, verringert seine Wirksamkeit bei der Bewältigung neuer oder anderer Herausforderungen in der Zukunft erheblich. Stattdessen sollten Pläne und Ergebnisse proaktiv überprüft und Business Continuity-Pläne regelmäßig aktualisiert werden. Nach einer schwerwiegenden Störung sollten Sie bewerten, wie gut der Plan in der Praxis funktioniert hat.

Die Überprüfung des Business Continuity-Plans ist ein aktiver Prozess, der eine Reihe von Schritten umfasst.

Tests und Vorbereitung

Es ist wichtig, dass Ihr Plan auf mögliche negative Auswirkungen geprüft wird. Ein nicht getesteter Plan ist fast so nützlich wie gar kein Plan. Ein regelmäßiger Testzyklus wird Lücken in Ihrem Plan aufdecken. Ein gründlich getesteter Plan gibt Ihnen die Flexibilität, auf sich ständig ändernde Bedrohungen zu reagieren.

Überprüfung der Wirksamkeit von Richtlinien und Verfahren

Prüfen Sie, ob die Richtlinien und Verfahren Ihren aktuellen Bedürfnissen entsprechen. Fragen Sie sich, ob sie unter den gegebenen Umständen, mit der verfügbaren Ausrüstung und dem verfügbaren Personal wirksam sind. Stellen Sie sich folgende Fragen:

- Erfüllen Ihre Verfahren noch ihre ursprünglichen Ziele?
- Was kann angepasst werden, um Änderungen seit der letzten Überprüfung (oder der ersten Version) des Plans zu berücksichtigen?
- Wenn Sie bereits mit einer größeren Bedrohung konfrontiert waren, haben die Richtlinien und Verfahren dem zuständigen Personal während des Ereignisses angemessenen Zugang und Kontrolle ermöglicht?
- Erfolgte die Kommunikation rechtzeitig und regelmäßig?

Software-Updates und Sicherheitspatch-Management

Es ist hilfreich, einen Plan für System-Updates und Patch-Management zu haben, aber beide Aufgaben müssen auch regelmäßig durchgeführt (und getestet) werden. Die Cybersecurity and Infrastructure Security Agency (CISA) führt eine Liste von routinemäßig ausgenutzten Software-Schwachstellen, die mit Software-Patches behoben werden können. Die CISA empfiehlt die Installation von Updates und Sicherheitspatches, sobald dies für Ihr Unternehmen möglich ist. MSPs bieten automatisierte Lösungen zur Verwaltung von Software-Updates und Patches an, um sicherzustellen, dass diese rechtzeitig installiert werden.

Umsetzung einer Zero-Trust-Richtlinie

Der Begriff Zero Trust bezeichnet ein Sicherheitsmodell, das die Bereitstellung und den Betrieb von Systemen regelt, die nach sogenannten Zero-Trust-Prinzipien entwickelt wurden. Das Zero-Trust-Modell wird eingesetzt, um vertrauliche Informationen, Systeme und Services zu schützen. Ein solches Zero-Trust-Modell geht davon aus, dass Datenschutzverletzungen unvermeidbar sind und möglicherweise bereits stattfinden. Bei diesem Sicherheitsansatz können Benutzer:innen nur auf die Informationen zugreifen, die sie gerade benötigen (Prinzip der geringsten Rechte). Alle Benutzerverbindungen werden überprüft, bevor sie fortgesetzt werden können. Die Durchsetzung einer Zero-Trust-Richtlinie ist nur auf Systemen möglich, die nach diesem Sicherheitsmodell konzipiert sind.

Mitarbeiterschulungen

Eine Schulung des IT-Personals ist ein wichtiger Aspekt bei Disaster Recovery- und Business Continuity-Plänen. Die Mitarbeiter:innen müssen ihre Rollen und Verantwortlichkeiten verstehen, die sie im Rahmen eines Kontinuitätsplans haben. Teamleiter:innen können Unterstützung und Schulungen anbieten und das Bewusstsein für den Plan unter ihren direkten Mitarbeiter:innen fördern. Mitarbeiter:innen, die mit dem Plan nicht vertraut sind, werden große Schwierigkeiten haben, ihn in einer Situation umzusetzen, in der die Zeit drängt.

Fazit

Serviceunterbrechungen und Katastrophen sind unvermeidlich – und Cyberkriminelle nehmen sogar die kleinsten Unternehmen ins Visier. Vereinfachen Sie die Cyber Protection für Ihr Unternehmen mit einer effizienten Cloud-basierten Komplettlösung, anstatt mehrere Tools für Endpunktsicherheit, Malware- und Virenschutz sowie Backup zu verwalten.

Schützen Sie Ihre Daten vor allen Bedrohungen mit Acronis Cyber Protect – der einzigen Cyber Protection-Lösung, die Data Protection und Cyber Security nahtlos integriert.

Seien Sie auf alle Arten von Störungen vorbereitet, unabhängig davon, wo diese ihren Ursprung haben. Die Cyber Protection Operation Centers (CPOCs) von Acronis bilden ein globales Sicherheitsnetzwerk, das Bedrohungen abwehrt und überwacht. Die Acronis CPOCs warnen Sie in Echtzeit vor Malware, Schwachstellen, Naturkatastrophen und anderen globalen Ereignissen, die sich auf Ihre Data Protection auswirken können.

Acronis

Weitere Informationen finden Sie auf www.acronis.com