AUSGABE 05

IT insider

TECHNIK. BUSINESS. TRENDS.

IT-INFRASTRUKTUR

Dem Desaster die Stirn bieten

IT-SERVICE .NETWORK

Sehr geehrte Damen und Herren, liebe Geschäftspartner,

grundsätzlich sollten Sie natürlich nicht immer mit dem Schlimmsten rechnen. Das hätte nämlich eine sehr negative Grundeinstellung zur Folge – und die könnte sich für Ihr Unternehmen (beziehungsweise Ihren Betrieb, Ihre Praxis, Ihre Kanzlei oder Ihre Einrichtung) als ein großes Hemmnis erweisen. Denn: Warum sollten Sie etwas Neues wagen und an Innovationen arbeiten, wenn das Ergebnis wahrscheinlich nicht zufriedenstellend ist? Nein, einen solchen Pessimismus schieben wir lieber beiseite und schaffen dadurch Platz für Entdeckergeist, Tatendrang und Mut!

Aber: Wenn Ihnen die Existenz Ihres Unternehmens am Herzen liegt, sollten Sie sich nichtsdestotrotz auf die Möglichkeit gewisser Katastrophen vorbereiten. So unwahrscheinlich es im Augenblick auch scheinen mag, so können doch einige Szenarien eintreten, die sich für Unternehmen als ein echtes Desaster erweisen können – vor allem, wenn sie keinen Plan haben, was in dem jeweiligen Szenario genau zu tun ist. Sie fragen sich: Was für Szenarien könnten das genau sein? Es könnte zum Beispiel zu einem Hochwasser, einem Brand, einem Stromausfall oder einer Cyberattacke kommen.

In dieser Ausgabe des Kundenmagazins ITinsider beschäftigen wir uns mit genau solchen Szenarien. Wir zeigen auf, welche Gefahren drohen und wie Sie im Fall der Fälle am besten reagieren. Außerdem erklären wir, wie sich Ihr Unternehmen schon im Vorfeld aufstellen sollte, um für die möglichen Szenarien gewappnet zu sein und so unbeschadet wie möglich daraus hervorzugehen. Kleiner Spoiler: Mit Maßnahmen und Lösungen wie einem Notfallkonzept, einer USV-Anlage, einer Datensicherung und der Netzwerksegmentierung können Sie vorbeugend schon viel tun.

Wenn Sie dieses Magazin nach der (vollständigen) Lektüre wieder aus der Hand legen, werden Sie wissen, warum Sie sich auf bestimmte Szenarien vorbereiten sollten – und wie Sie dem Desaster im Ernstfall die Stirn bieten. Und Sie werden wissen, wie wir Ihnen bei all dem helfen können. Sollten Sie spezifische Fragen haben oder sich gemeinsam mit uns für Katastrophen wappnen wollen, sind wir gern für Sie da!

Wir wünschen Ihnen viel Spaß beim Lesen!

Ihr Systemhaus

INHALT

IMPRESSUM

Herausgeber
SYNAXON AG | Falkenstraße 31 | D-33758 Schloß Holte-Stukenbrock
Telefon 05207 9299 – 200 | Fax 05207 9299 – 296
E-Mail info@synaxon.de | www.synaxon.de
Redaktion
André Vogtschmidt (V.i.S.d.P.), Janina Kröger
Ansprechpartner
André Vogtschmidt | andre.vogtschmidt@synaxon.de

Konzept / Gestaltung
Mirco Becker
Druck
Wentker Druck GmbH
Gutenbergstraße 5 – 7 | 48268 Greven
www.wentker-druck.de

Wir drucken klimaneutral mit natureOffice

FSC www.fsc.org 100% From well-managed forests FSC® C000000

Stand 04/2022. Irrtümer und Druckfehler vorbehalten. Bildnachweise stock.adobe.com: # 129782231 © Syda Productions; # 289516021 © Robert Kneschke; # 71176227 © Jag_cz; # 378075987 © Svitlana; # 32995789 © twystydigi; # 452878956 © Gorodenkoff; # 312266188 © rangizzz; # 456902532 © SHOTPRIME STUDIO; # 461427061 © k_yu; # 242021653 © lassedesignen

Bieten Sie Desastern die Stirn!

Ein Brand zerstört das Firmengebäude, ein Hochwasser setzt alles unter Wasser, ein regionaler Stromausfall dreht dem Unternehmen den Saft ab oder eine Cyberattacke sorgt für einen IT-Ausfall – es gibt einige Szenarien, die für Unternehmen ein Desaster bedeuten. Häufig geht es um nicht weniger als die Existenz.

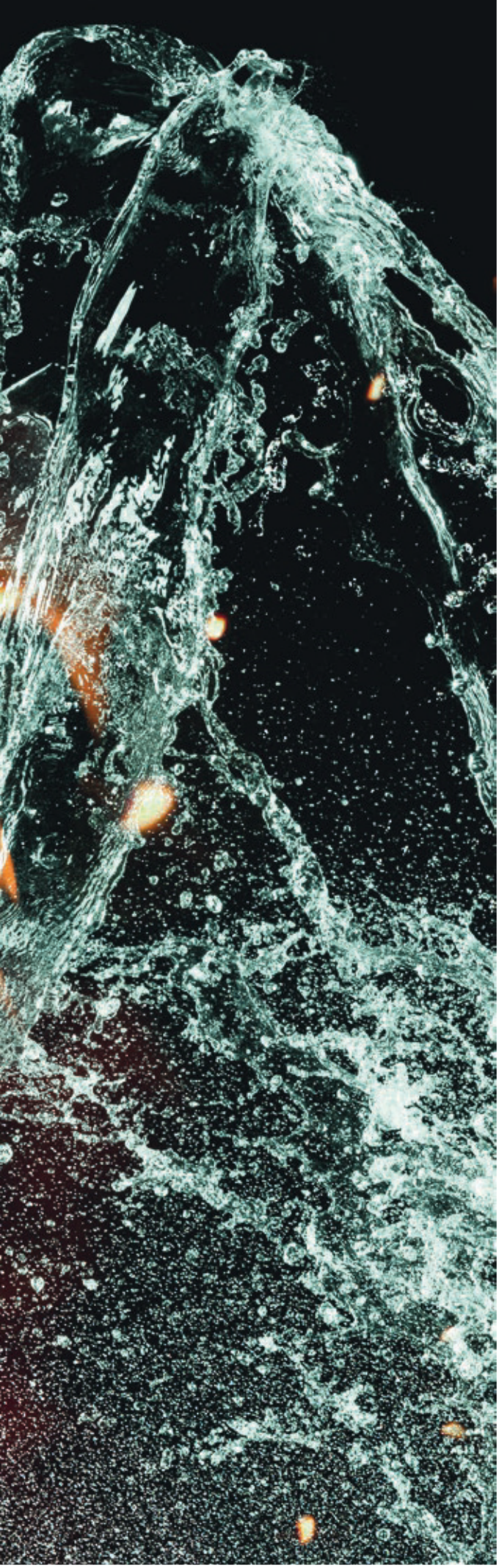
Katastrophen kommen unverhofft

Natürlich gehen Sie davon aus, dass alles wie gewohnt seiner Wege geht. Manchmal tritt das Unverhoffte aber doch ein. Das Jahr 2021 hat dafür ein eindrucksvolles Negativbeispiel gebracht: Bei der Hochwasserkatastrophe im Juli starben in Teilen Deutschlands mehr als 180 Menschen, tausende Existenzen wurden zerstört. Auch viele Unternehmen wurden von der Hochwasserkatastrophe hart getroffen: Stillgelegte Produktionsanlagen, verwüstete Werke und Geschäfte, überflutete Lagerhallen und zerstörte Infrastrukturen – das Hochwasser hat in der Unternehmenslandschaft der betroffenen Regionen eine Spur der Verwüstung gezogen und viele Existenzen bedroht.

So unwahrscheinlich es auch erscheint, dass eine solche Naturkatastrophe auch Ihr Unternehmen ereilt: Vorbereiten sollten Sie sich für den Fall einer massiven Störung Ihrer Betriebsabläufe dennoch. Immerhin gibt es auch andere Szenarien, die unter Umständen eine genauso große Katastrophe bedeuten können. Fällt zum Beispiel die Stromversorgung in der Region aus, stehen Produktionsanlagen still. Ein Firmenbrand ist aus allen möglichen Gründen denkbar. Und eine der größten Gefahren für Unternehmen lauert dank der Umtriebigkeit der Cyberkriminellen oft nur einen Mausklick entfernt.

Auf das Desaster vorbereiten

Genau deshalb ist es so wichtig, dass sich Unternehmen mit verschiedenen »Was wäre, wenn«-Konstellationen beschäftigen und sich genau überlegen, wie in welchem Katastrophenfall zu reagieren ist.



Denn das ist selbstverständlich: Je länger eine Betriebsstörung andauert, desto teurer wird sie für das Unternehmen. Störungen können nämlich zu Umsatzeinbußen, Imageschäden und Unzufriedenheit seitens der Kunden führen – und die Quittung dafür lässt meist nicht lange auf sich warten. Es gilt also, das Problem schnellstmöglich unter Kontrolle zu bekommen und den Schaden in Grenzen zu halten.

Am besten ist es, wenn Unternehmen genaue Pläne für derartige Szenarien in der Hinterhand haben. Solche Pläne helfen nämlich maßgeblich dabei, den Kopf nicht zu verlieren, Schritt für Schritt die anstehenden Aufgaben anzugehen und abzuarbeiten und dadurch so zügig, aber durchdacht wie möglich das Problem oder die Krise zu bewältigen und dabei die Geschäftstätigkeit irgendwie aufrecht zu erhalten – was im Fall der Hochwasserkatastrophe aber in vielen Fällen schlicht nicht möglich war. Für diese Art des Vorgehens gibt es natürlich auch einen Fachbegriff: Business Continuity.

So schnell wie möglich vom Desaster erholen

Die IT spielt in solchen Szenarien grundsätzlich eine besonders wichtige Rolle. Denn: Ob Wasserschaden, Brand, Stromausfall oder Cyberangriff – die IT-Infrastruktur gerät fast immer in Mitleidenschaft. Zudem bildet sie für immer mehr betriebliche Prozesse die Grundlage. In der Fertigung arbeiten immer mehr Maschinen computergesteuert; Kundenanfragen gehen in einigen Branchen fast nur noch online ein; die geschäftliche Kommunikation läuft fast ausschließlich elektronisch ab; und für die Logistikplanung stellen elektronische Systeme inzwischen ebenfalls den Dreh- und Angelpunkt dar.

Während es bei der Business Continuity um die Aufrechterhaltung kritischer Geschäftsabläufe und die Sicherstellung der Geschäftstätigkeit im Allgemeinen geht, fokussiert sich Disaster Recovery auf die Wiederherstellung von IT-Services. Der Begriff lässt sich mit Notfall- oder Katastrophenwiederherstellung ins Deutsche übersetzen. Im Rahmen von Disaster Recovery gilt es zum Beispiel, Server, Netzwerke, Telefonanlagen oder Datenspeicher wiederherzustellen.

So bieten Unternehmen Desastern die Stirn

Damit Unternehmen im Fall der Fälle schnell reagieren können und handlungsfähig bleiben, gibt es im Vorfeld einiges zu organisieren. Zum Beispiel: Mit einem System zur unterbrechungsfreien Stromversorgung lässt sich sicherstellen, dass unternehmenskritische Bereiche auch bei einem regionalen Stromausfall weiterbetrieben werden können; mit einem Desaster-Recovery-Plan beziehungsweise IT-Notfallplan liegen To-Do-Listen für den Ernstfall bereit; mit einer umfassenden Datensicherung inklusive einer fern des Firmenstandorts hinterlegten Kopie können weder Naturkatastrophen noch Cyberattacken Unternehmensdaten etwas anhaben; und mit einer durchdachten Netzwerksegmentierung sind besonders wichtige Netzwerkbereiche und Unternehmensdaten bestens geschützt.

Auf den folgenden Seiten werden wir auf die angerissenen Themen jeweils im Detail eingehen und erklären, warum welche Maßnahmen in welchen Fällen so wichtig sind. Außerdem werden wir darlegen, wie wir Ihnen als IT-Dienstleister dabei helfen können, sich auf Katastrophen jedweder Art vorzubereiten und Desastern die Stirn zu bieten. Sollten Fragen dazu offen bleiben, können Sie uns natürlich jederzeit dazu ansprechen. Wir beraten Sie immer gern!

Schritt für Schritt die Krise im Griff

Kommt es in einem Unternehmen zu einem Problem, zählt jede Sekunde. Es gilt, direkt zu reagieren, Ausfallzeiten zu minimieren und finanzielle Schäden einzugrenzen. Genau dafür gibt es diverse Leitfäden: Schritt für Schritt führen sie gezielt zurück zur Normalität.

Wenn Krisen Unternehmen erschüttern
Wissen Sie, was genau zu tun ist, wenn es in Ihrem Unternehmen zu einem Notfall kommt – sei es ein kompletter Stromausfall, ein durch einen Cyberangriff ausgelöster IT-Ausfall oder ein Wasserschaden im Gebäude? Sollten Sie diese Frage mit einem »Ja« beantworten, liegen vermutlich diverse Leitlinien und Handlungsanweisungen für Notfälle jeglicher Art griffbereit in Ihrer Schublade. Falls Ihnen dagegen ein »Nein« auf der Zunge liegt, ist es dringend an der Zeit, aktiv zu werden.

Warum? Ganz einfach: Weil konkrete Handlungsanweisungen dabei helfen, auf jedes nur denkbare Szenario umgehend und angemessen zu reagieren. So lässt sich das Problem schnell in den Griff bekommen und im Idealfall kehrt – ohne großartige zeitliche und finanzielle Verluste – bald wieder Normalität ein. Das Problem ist: Sie können solche Leitfäden nicht einfach im Internet suchen, ausdrucken und fertig ist die Sache. Vielmehr ist einige Vorarbeit notwendig, damit Ihr Unternehmen auf jeden Notfall perfekt vorbereitet ist.

Das Notfallhandbuch ist individuell
Gebündelt werden solche Leitfäden in einem Notfallhandbuch. Nach der Definition des Bundesamts für Sicherheit in der Informationstechnik (BSI) hat so ein Handbuch ganz besonders die Fortführung der Geschäftsprozesse (Business Continuity) im Blick. Daher sind vor allem zwei Dokumente wichtig: die Geschäftsfortführungspläne und die Wiederanlaufpläne. Hinzu können aber noch einige weitere Dokumente kommen, darunter ein Plan für Sofortmaßnahmen, ein Krisenstabsleitfaden und ein Krisenkommunikationsplan.

Aber warum gibt es so ein Notfallhandbuch nicht fertig zum Ausdrucken? Der Grund ist einfach: Jedes Unternehmen ist anders gestrickt – und daher muss auch jedes Notfallhandbuch individuell erstellt werden. Es sind beispielsweise spezielle Abläufe, bauliche Voraussetzungen, konkrete Ansprechpartner, besondere Prioritäten et cetera zu berücksichtigen. Hinzu kommt, dass es verschiedene Möglichkeiten gibt, ein Notfallhandbuch aufzubauen.

BSI gibt Tipps für Leitfäden
Denkbar ist zum Beispiel ein Aufbau nach den Phasen des Notfall-Managements. Grob handelt es sich dabei um das Erkennen und Melden des Notfalls, das Ergreifen von Sofortmaßnahmen, die Geschäftsfortführung, den Wiederanlauf sowie die Wiederherstellung und schließlich die Rückführung vom Not- zum Normalbetrieb und die Nachbearbeitung. Genauso gut ist aber auch eine Gliederung nach Verantwortungsebenen und -bereichen oder eine Einteilung nach Prozessen möglich.

Grundsätzlich lässt sich festhalten: Ein modularer Aufbau ist in jedem Fall sinnvoll, denn dadurch kann jeder Mitarbeiter schnell den für ihn relevanten Bereich finden und entsprechend der Anweisungen agieren. Unser Tipp: Der BSI-Standard 100-4 kann Unternehmen bei der Erarbeitung eines Notfallhandbuchs wichtige Hilfestellungen bieten.

Mit IT-Notfallhandbuch Krisen bewältigen
Ein wichtiges Element im Notfallhandbuch ist im Übrigen auch der IT-Notfallplan. Dieser fokussiert sich – der Name lässt es schon vermuten – speziell auf IT-Notfälle beziehungsweise IT-Ausfälle und hat letztlich dasselbe Ziel: Die Krise soll so schnell und effizient wie möglich überwunden und der Normalzustand wiederhergestellt werden. Gern helfen wir Ihnen dabei, einen solchen IT-Notfallplan zu erstellen. Damit Sie schon einmal wissen, was Sie bei diesem Plan genau erwartet, stellen wir Ihnen den IT-Notfallplan und seine Besonderheiten in der unten stehenden Box etwas genauer vor.

IT-Notfallplan – für IT-Ausfälle gewappnet

Der IT-Notfallplan ist Teil des Notfallhandbuchs. In ihm ist festgehalten, wie trotz eines Störfalls auf wichtige Informationen zugegriffen werden kann, wie sich die Informationssicherheit im Notfall aufrecht erhalten lässt und wie der IT-Betrieb nach einer Störung schnell und zielgerichtet wiederhergestellt werden kann.

Die IT-Dokumentation bildet dafür die wichtigste Grundlage. Sie enthält unter anderem Informationen über Hardware und Peripherie-Geräte, Software-Anwendungen, IP-Adressen, VPN- und Serverzugänge sowie E-Mail-/Exchange-Daten. Neben der IT-Dokumentation sollten sich Personallisten mit Kontaktdaten, Alarmierungspläne und Meldewege, Beschaffungsprozesse für den Notfall, Maßnahmen zur Beendigung und Dokumentation des Notfalls, Notfallvorsorgepläne und Wiederherstellungspläne für alle Anlagen im IT-Notfallplan befinden.


DEMO
ONLY
TOP
DESSUS
NUCA

Immer unter Strom

Die Stromversorgung ist fast schon so etwas wie die Achillesferse eines Unternehmens. Denn: Wenn wortwörtlich die Lichter aus sind, lassen sich keine Geschäfte machen. Daher existiert die unterbrechungsfreie Stromversorgung. Sie stellt zuverlässig sicher, dass Unternehmen immer unter Strom stehen.

Gefahr durch Stromausfälle

Fakt ist: In Deutschland sind Stromausfälle eher selten. Von 15,14 Minuten im Jahr 2017 ist die durchschnittliche Unterbrechungsdauer auf 10,73 Minuten im Jahr 2020 gesunken. Dennoch kommen Stromausfälle vor. Im September 2021 gingen beispielsweise in 300.000 Haushalten in Dresden die Lichter aus, kurz darauf waren 20.000 Einwohner in Wiesbaden zeitweise ohne Strom. Betroffen sind von solchen Ausfällen nicht nur Privatleute, sondern auch Unternehmen.

Und das kann kostspielige Folgen haben. In Dresden hat diese Erfahrung die Chipfabrik Infineon machen müssen. Aufgrund des regionalen Stromausfalls musste die Produktion gestoppt werden, die Schäden dadurch lagen im Millionenbereich. Problematisch ist in einem solchen Szenario nicht nur der Produktionsstopp; möglicherweise können bei einem plötzlichen Ausfall wichtige Daten nicht gespeichert werden und gehen verloren. Auch dadurch können für Unternehmen Schäden entstehen, an denen sie langfristig zu knapsen haben.

Drohen Blackouts in Deutschland?

Als wäre das nicht schon genug, werden jetzt auch noch Szenarien mit großflächigen Blackouts heraufbeschworen. Faktoren, die dafür sprechen, gibt es mehrere. Niedrige Erdgasreserven gehören dazu, genauso wie die Abschaltung von immer mehr Atom- und Kohlekraftwerken. Die zunehmende Abhängigkeit von regenerativen Energien tut ihr Übriges dazu, denn längere Zeiträume, in denen kein Wind weht und auch keine Sonne scheint, könnten zu einem Ungleichgewicht im Stromnetz und damit zu Ausfällen führen. Denn: Wenn weniger elektrische Energie in ein Stromnetz eingespeist als verbraucht wird, geht die Rechnung irgendwann nicht mehr auf.

Und dann könnte noch eine weitere Bedrohung auf der Bildfläche erscheinen: Hacker nehmen zunehmend kritische Infrastrukturen (KRITIS) in den Blick – und dazu gehört nun einmal auch die Stromversorgung. Derartige Angriffe auf das deutsche Stromnetz gab es in der Vergangenheit bereits, bisher blieben sie aber ohne Konsequenzen für dessen Stabilität. Doch das ist keine Selbstverständlichkeit: Die steigenden Zahlen an Cyberangriffen versetzen uns in erhöhte Alarmbereitschaft. Deshalb ist es umso wichtiger, derartigen Angriffen auf Energieversorgungsquellen effektiv vorzubeugen.

Auf den Ernstfall vorbereiten

Behörden wie auch Stromversorger nehmen die Möglichkeit eines Cyberangriffs auf das Stromnetz dementsprechend ernst. Stromnetzbetreiber sind daher unter anderem dazu verpflichtet, Systeme zur

Die drei Klassen von USV-Anlagen

- **Standby- oder Offline-USV**
  Diese einfachste und günstigste Klasse von USV-Anlagen bietet den geringsten Schutz. Lediglich gegen Netzausfälle und kurzzeitige Spannungsspitzen sind Unternehmen dadurch abgesichert. Unter- und Überspannungen lassen sich damit nicht ausgleichen.

- **Line-Interactive / Netzinteraktive USV**
  Diese Klasse von USV-Anlagen schützt vor Netzausfällen und kurzzeitigen Spannungsspitzen und kann zudem durch den Einsatz von Filtern dauerhaft Spannungsschwankungen regulieren. Dadurch eignen sich Netzinteraktive USV besonders für Gegenden, in denen Spannungsschwankungen häufig vorkommen.

- **Online- / Dauerwandler-USV**
  Während bei den beiden anderen Klassen die Last erst bei einem Netzausfall auf den Batteriebetrieb geschaltet wird und dadurch eine Umschaltzeit entsteht, gelten Online-USV-Anlagen als echte Stromgeneratoren. Sie erzeugen dauerhaft eine eigene Netzspannung und können die angeschlossenen Stromverbraucher ohne Einschränkungen mit einer gleichbleibenden Netzspannung versorgen; zeitgleich wird die Batterie aufgeladen.

Angriffserkennung einzusetzen. Aber: Das Bundesamt für IT-Sicherheit in der Informationstechnik (BSI) geht davon aus, dass es trotz aller Präventionsmaßnahmen dennoch irgendwann zu einem erfolgreichen Angriff kommen könnte. Und das wiederum bedeutet, dass sich auch Unternehmen auf die Eventualität eines Stromausfalls einstellen müssen – sei es durch einen Hackerangriff oder aber durch einen Kabelfehler oder Kurzschluss in einem Umspannwerk.

Genau hier kommt die unterbrechungsfreie Stromversorgung – kurz: USV – ins Spiel. USV-Anlagen sind dazu da, im Falle eines Ausfalls des regionalen Stromnetzes die Stromversorgung sensibler IT-Systeme in Unternehmen sicherzustellen und kurzzeitige Unter- und Überspannungen abzufangen. Denn: Durch derartige Störungen können Schäden an elektrischen Geräten entstehen – und das schließt auch die Firmen-IT mit ein. Das grundsätzliche Ziel der unterbrechungsfreien Stromversorgung ist es also, die Energieversorgung für eine bestimmte Zeit aufrecht zu erhalten – bis die Notstromaggregate anspringen.

USV-Anlagen sichern die Business Continuity

Damit verhindern Anlagen zur unterbrechungsfreien Stromversorgung – häufig in Kombination mit Netzersatzanlagen – nicht nur Schäden an elektrischen Geräten, sondern sichern auch die Business Continuity von Unternehmen. Und weil sie in diesem Zuge auch dafür sorgen, dass keine wichtigen Unternehmensdaten verloren gehen, spielen sie auch aus Sicht des Datenschutzes eine wichtige Rolle. Sofern Sie in Ihrem Unternehmen noch keine solche Anlage einsetzen, sollten Sie also definitiv darüber nachdenken – schließlich ist der Nutzen am Ende des Tages enorm. Sollten Sie sich für eine Anschaffung entscheiden, gibt es allerdings einiges zu bedenken.

Denn: Es gibt verschiedene Varianten von USV, der Bedarf richtet sich vor allem nach der Größe und den Anforderungen eines Unternehmens. Es gilt, den genauen Bedarf abzustecken und die Angebote zu vergleichen. Sie benötigen Hilfe dabei? Dann sprechen Sie uns an – wir helfen Ihnen gern bei der Auswahl und Installation!

Rückendeckung durch Rechenzentren

Viele Unternehmen greifen auf Rechenzentren zurück, um ihre Daten in einer rund um die Uhr überwachten Umgebung aufzubewahren. Dabei müssen sie sich auf den zuverlässigen Betrieb des Rechenzentrums verlassen können. Neue Technologien stellen das sicher.

Wohin mit den Unternehmensdaten?
Bei so ziemlich jeder unternehmerischen Handlung, die am PC ausgeführt wird, werden Daten verarbeitet. E-Mails werden empfangen, beantwortet und archiviert; Kundendaten werden aufgerufen, verwendet und vielleicht mit einer Notiz versehen; Präsentationen werden erstellt, vorgeführt und mit Zugriff für die Zuhörer abgespeichert. Tag für Tag werden dadurch neue Daten produziert und die Datenberge wachsen. Teilweise geschieht das so schnell, dass sich Unternehmen überfordert fühlen.

Schließlich ist der Betrieb eigener Server oder eines eigenen (kleinen) Rechenzentrums keine einfache Sache. Warum? Weil auch hier das ein oder andere Desaster droht. Zum Beispiel weil technische Komponenten Wärme erzeugen und es zu einer Überhitzung und in der Folge zu einem Ausfall kommen könnte. Möglich ist auch, dass Daten durch einen regionalen Stromausfall verloren gehen. Und dann gibt es noch physische Gefahren wie einen Brand, die es frühzeitig zu erkennen gilt. Sie sehen: Der Betrieb eines eigenen Rechenzentrums stellt vor allem kleinere Unternehmen vor eine Herausforderung. Aber was ist die Lösung?

Externe Rechenzentren helfen weiter!
Um nicht selbst ein (kleines) Rechenzentrum betreiben zu müssen, entscheiden sich viele Unternehmen, die Dienste eines externen Rechenzentrums in Anspruch zu nehmen und dafür zu zahlen, dass ihre Daten in einer sicheren, rund um die Uhr bewachten, temperaturkontrollierten Einrichtung hinterlegt sind. Denn: Professionelle Rechenzentren sind allesamt mit Umgebungskontrollsystemen, Energieversorgungssystemen und Sicherheitstechnik ausgestattet. Dadurch soll nicht nur der störungsfreie Betrieb des Rechenzentrums sichergestellt werden; diese speziellen Infrastruktur-Komponenten sorgen auch dafür, dass sich Unternehmenskunden auf die Sicherheit ihrer wichtigen Daten verlassen und zu jeder Zeit darauf zugreifen können.

Im Grundsatz ähnelt sich der Aufbau solcher Rechenzentren stark. Sie verfügen über Server-Hardware, aktive und passive Netzwerk-Komponenten und Baugruppenträger; und eben über die bereits erwähnten Infrastruktur-Komponenten, die den störungsfreien Betrieb absichern. Es gibt aber auch deutliche Unterschiede zwischen den verschiedenen Betreibern von Rechenzentren. Bei der Entscheidung für ein Rechenzentrum lohnt es sich für Unternehmen daher durchaus, auf die Details zu achten. Denn: Ihre Zukunft hängt auch von der Sicherheit ihrer Daten ab.

Nicht auf Strom verlassen
Auch der bekannte US-amerikanische Halbleiterhersteller Intel® stellt als Anbieter Rechenzentrumsleistungen für Kunden bereit – und geht beim Betrieb seiner Rechenzentren einen ganz neuen Weg. Hintergrund dessen ist die bis dato existierende enorme Abhängigkeit vom öffentlichen Stromnetz als primäre Stromversorgungsquelle. Die Gefahr von Stromausfällen, Spannungsstörungen und Frequenzschwankungen wollte Intel® als Betreiber eines Rechenzentrums nicht länger hinnehmen und hat sich daher nach Alternativen umgesehen.

Dabei ist der Blick unter anderem auch auf die Brennstoffzellentechnologie gefallen. Das Potenzial dieser Technologie hinsichtlich der Steigerung der Betriebseffizienz, Produktivität und Nachhaltigkeit schien vielversprechend und so entschied sich Intel® dazu, die Technologie im eigenen Rechenzentrum im indischen Bangalore mit einer Fallstudie auf Herz und Nieren zu testen. Mit Erfolg: Die Brennstoffzellentechnologie hat sich als eine zuverlässige, stabile, effiziente und nachhaltige Energiequelle für Rechenzentren erwiesen.

Intel® setzt auf Brennstoffzellen
Im Intel®-Rechenzentrum in Santa Clara, USA, wurde noch eine zweite Fallstudie durchgeführt und auch hier konnte die Brennstoffzellentechnologie – in einer leicht abweichenden Umsetzung – überzeugen. Dabei bestätigte sich auch eine interessante Erkenntnis der Fallstudie aus Bangalore: Die Stromversorgung des Rechenzentrums direkt aus den Brennstoffzellen ist so zuverlässig, dass eine USV-Anlage überflüssig ist. Stattdessen wird ein UPCM (Uninterruptible Power Conditioning Module; unterbrechungsfreies Stromkonditionierungsmodul) installiert. Dadurch werden geschützte Verbraucher bei Netzausfällen oder -störungen mit konstantem Strom versorgt.

Aber die zuverlässige Stromversorgung ist für Intel® nicht das einzige Argument, das für die Brennstoffzellentechnologie spricht. Als zusätzliche Vorteile haben sich die geringeren Emissionen im Vergleich zu Dieselgeneratoren für die Notstromerzeugung und ein geringerer Flächenverbrauch im Vergleich zu herkömmlichen Umspannwerken erwiesen – und das ist gut für die Nachhaltigkeit. Für Intel® steht daher fest: Sofern es möglich ist, wird die Brennstoffzellentechnologie beim Design künftiger Rechenzentren zum Einsatz kommen.

Info: Brennstoffzellentechnologie

Schon im Jahr 1839 ist die erste Brennstoffzelle erfunden worden. Seitdem hat sich die Brennstoffzellentechnologie zwar stark weiterentwickelt, die Grundidee ist aber dieselbe geblieben: Zwei Elektroden – eine negative Elektrode (Anode) und eine positive Elektrode (Kathode) sind dabei um einen Elektrolyten herum angeordnet. Das Ergebnis dessen ist, dass eine Brennstoffzelle durch eine elektrochemische Reaktion Strom erzeugt – und zwar dadurch, dass Brennstoff und Luft gemischt werden, wodurch Strom und Wasser verbrennungslos erzeugt werden. Neben Wasserstoff können heute auch Propan, Erdgas und Biogas als Brennstoff genutzt werden. Intel® setzt beim Betrieb seiner Rechenzentren auf Erdgas als Brennstoff. Die Brennstoffzellen im Rechenzentrum in Bangalore dienen inzwischen sogar als die primäre Energiequelle, während das eigentliche Stromnetz nur noch als Backup genutzt wird.

Ein Cyber-angriff: aus die Maus?

Cyberangriffe gelten inzwischen als die größte Gefahr für Unternehmen – noch vor Betriebsunterbrechungen, Naturkatastrophen und Pandemien. Aber ist bei einem erfolgreichen Cyberangriff wirklich direkt alles verloren? Wie gilt es im Ernstfall zu reagieren? Ist eine Schadensbegrenzung möglich?

Cybercrime: Prognosen sind düster

Der BSI-Bericht zur Lage der IT-Sicherheit in Deutschland kommt eigentlich jedes Jahr wieder zu demselben Ergebnis: Das Cybercrime-Geschehen ist auf einem neuen Höchststand. Geht es nach einigen Branchenexperten, ist die aktuelle, bereits als kritisch einzustufende Lage aber nur der Anfang: Befürchtet wird demnach in den kommenden Jahren eine Cybercrime-Welle unvorstellbaren Ausmaßes. Künftige Attacken könnten noch mehr Potenzial haben, Unternehmen zu ruinieren und kritische Infrastrukturen (KRITIS) zu (zer-)stören. Das bedeutet: Jedes Unternehmen muss darauf vorbereitet sein, jederzeit Ziel eines Angriffs mit oft unkalkulierbaren Folgen zu werden.

Das alles klingt vielleicht erstmal sehr stark nach einer Hypothese. Aber was ist, wenn das Szenario eines Cyberangriffs tatsächlich eintritt? Ist dann direkt alles verloren? Oder gibt es irgendwelche Möglichkeiten, mit denen sich die potenziell existenzbedrohenden Auswirkungen eines erfolgreichen Hackerangriffs eingrenzen lassen? Wichtig ist in so einem Fall zuallererst eines: Betroffene Unternehmen müssen bedacht, aber schnell auf die heikle Situation reagieren.

Hackerangriff: im Ernstfall richtig handeln

Vor allem für die Ursachenforschung ist es wichtig, Ruhe zu bewahren, sobald ein Hackerangriff bemerkt worden ist. Denn: Ein unüberlegtes und überstürztes Handeln könnte wichtige Angriffsspuren vernichten. Ein vorschneller Reset, also ein Neustart der Systeme, könnte zum Beispiel dafür sorgen, dass eigentlich wichtige Spuren plötzlich verwischt sind. Nichtsdestotrotz ist ein schnelles Handeln elementar: Unverzüglich sollten IT-Experten hinzugezogen werden, die in einer solchen Situation helfen können. Das kann beispielsweise ein externer IT-Dienstleister – zum Beispiel wir – sein, der aus seinen Mitarbeitern ein Incident-Response-Team zusammenstellt. In Rücksprache mit den Experten sind dann auch umgehend die Systeme fachgerecht abzuschalten. Im Prinzip handelt es sich hierbei um einen Wettlauf mit der Zeit – beziehungsweise mit den Hackern. Eventuell lässt es sich nämlich noch verhindern, dass sich die Angreifer in den Systemen ausbreiten und/oder Daten verschlüsseln.

Sind die Systeme einmal abgeschaltet, geht die Arbeit der Experten erst so richtig los. Zunächst müssen sie das Einfallstor der Angreifer ausfindig machen und bewerten, welche Systeme genau von dem Angriff betroffen sind – dabei kann unter anderem das Netzwerk-Monitoring wichtige Erkenntnisse liefern. Die Experten prüfen in diesem Zuge auch, ob und in welchem Umfang Daten entwendet worden sind.

Mit Cyberversicherung absichern

Die Investition in ausgefeilte Sicherheitsmaßnahmen ist immer der beste Schutz vor Cyberangriffen. Zusätzlich macht es für Unternehmen aber auch Sinn, eine Cyberversicherung abzuschließen. Sie ist dazu da, im Schadensfall die finanziellen Folgen für den Geschädigten zu begrenzen. Zu den Standardleistungen der meisten Cyberversicherungen gehören:

- Entschädigung bei wirtschaftlichen Verlusten durch Betriebsausfälle
- Erstattung der Kosten für Daten- und Systemwiederherstellung
- Übernahme von Drittschäden (z. B. Schadensersatzforderungen durch Kunden)
- Bezahlung der Kosten für den Einsatz von IT-Forensik-Experten zur Analyse, Beweissicherung und Schadensbegrenzung
- Erstattung der Kosten für eine Rechtsberatung durch Anwälte für IT- und Datenschutzrecht bei Datenschutzverstößen
- Bezahlung der Kosten für PR-Spezialisten für Krisenkommunikation zur Eindämmung des Image-Schadens

Sämtliche Beweise – darunter Systemprotokolle, Logfiles, Datenträger, Notizen und eventuell auch Screenshots – werden währenddessen erfasst und gesichert. Das genaue Vorgehen der gesamten Analyse inklusive der Ergebnisse sollte Schritt für Schritt dokumentiert werden – für die Aufarbeitung des erfolgten Cyberangriffs und die sogenannte IT-Forensik können sich diese Informationen später noch als sehr wichtig erweisen.

Für die Zukunft besser aufgestellt

Parallel zur Ursachenforschung sind noch zwei andere Aufgaben wichtig. Erstens: Sollte es im Zuge des Cyberangriffs zu einem Datenschutzvorfall gekommen sein, ist die zuständige Aufsichtsbehörde umgehend zu informieren; laut der europäischen Datenschutzgrundverordnung (DSGVO) besteht in solchen Fällen nämlich eine Meldepflicht. Zweitens: Unternehmen sollten den Vorfall nach Außen so kommunizieren, dass die eigene Reputation möglichst wenig Schaden nimmt; PR-Experten können dabei unterstützen.

Hier empfiehlt es sich vor allem, grundsätzlich bei der Wahrheit zu bleiben. Sollte sich zu einem späteren Zeitpunkt herausstellen, dass Tatsachen verschwiegen oder beschönigt worden sind, leidet das Image des Unternehmens noch mehr, als es ohnehin schon durch den erfolgreichen Hackerangriff der Fall ist.

Nachdem die Angreifer und ihre Werkzeuge spurlos aus den Systemen verbannt und diese wiederhergestellt worden sind, geht es zuletzt noch an die Aufarbeitung des Vorfalls. Der wichtigste Punkt dabei: Betroffene Unternehmen müssen prüfen, ob die bereits eingesetzten Sicherheitsmaßnahmen ausreichen oder ob die IT-Sicherheit noch ausbaufähig ist. Dies ist besonders wichtig, um einerseits das Vertrauen von Geschäftspartnern und Kunden wieder aufzubauen und um andererseits in Zukunft nicht erneut Opfer eines Angriffs zu werden. Bei all diesen Herausforderungen und Aufgaben unterstützen wir Sie als professioneller IT-Dienstleister. Gern vermitteln wir Ihnen auch eine passende Cyberversicherung (siehe Kasten).

Backup: das Must-have in der Hinterhand

Alle Unternehmensdaten weg – ein absolutes Horrorszenario. Das Problem: So unwahrscheinlich ist ein solcher Vorfall leider nicht. Bedrohungen für Ihre Daten kommen nämlich aus vielen Richtungen. Da hilft es nur, ein Backup in der Hinterhand zu haben.

Und plötzlich sind die Daten weg

Vielleicht halten Sie es für unwahrscheinlich, dass Ihre Unternehmensdaten auf irgendeine Weise verloren gehen könnten. Die schlechte Nachricht ist aber, dass die Wahrscheinlichkeit eines Datenverlusts gar nicht so gering ist. Die größte Gefahr stellt technisches Versagen dar – sprich: ein Hardware-Schaden. Sei es eine Festplatte, die plötzlich nicht mehr funktioniert oder ein Server, der von einem Moment auf den anderen defekt ist. Menschliches Versagen kann genauso die Ursache für einen Datenverlust sein: Aus Versehen werden Daten überschrieben oder gelöscht und können danach nicht wieder aufgerufen werden.

Ebenfalls zu den größten Gefahren für Unternehmensdaten gehört fehlerhafte Software. Auch sie kann gravierende Datenverluste hervorrufen; und wird ein Update installiert, können dabei noch nicht gespeicherte Daten verloren gehen. Höhere Gewalt stellt eine weitere Ursache für einen Datenverlust dar. Hochwasser-, Sturm- und Brandschäden sind schwer vorhersehbar und noch schwerer zu beeinflussen, haben aber die Macht, sämtliche Unternehmensdaten zu zerstören. Zuletzt wären noch Cyberangriffe zu nennen, in erster Linie mit Ransomware. Von Jahr zu Jahr wird die Gefahr einer solchen Attacke größer: In den Jahren 2019/2020 waren nach Angaben des Branchenverbands Bitkom drei Viertel der deutschen Wirtschaft davon betroffen.

Dem Datenverlust vorbeugen

Problematisch sind Datenverluste besonders deshalb, weil Daten inzwischen als das wichtigste Gut eines Unternehmens gehandelt werden. Häufig ist daher auch vom »Öl des 21. Jahrhunderts« die Rede. Daten gelten heutzutage als Treibstoff für einen Großteil der Geschäftsprozesse in einem Unternehmen – und ohne Treibstoff kommt eine Maschine nicht in Gang. Dieses Bild lässt sich auf Unternehmen aus vielen Branchen übertragen. Denn: Unabhängig davon, ob es sich um einen kleinen oder mittelständischen Betrieb, eine Arztpraxis oder eine Rechtsanwaltskanzlei handelt, ist nichts daran zu rütteln, dass die Abhängigkeit von einer ständigen Datenverfügbarkeit enorm ist.

Unternehmen sind daher sehr gut beraten, einem Datenverlust so gut wie möglich vorzubeugen – und zwar mit einer zuverlässigen Datensicherung, auch Backup genannt. Falls Ihnen der Begriff unbekannt sein sollte: Als Backup werden Sicherheitskopien bezeichnet, mit denen sich Daten im Falle eines Verlusts wiederherstellen lassen. Allerdings gibt es für Unternehmen einiges zu beachten, damit sie sich auf ihr Backup in der Hinterhand auch wirklich verlassen können.

3-2-1-Regel für effektive Backups

Die sogenannte 3-2-1-Regel ist für Backups fast schon Gesetz. Sie gilt heute sozusagen als goldene Regel der Datensicherheit. Die Formel ist im Grunde genommen recht einfach: Sie besagt, dass drei Kopien oder Versionen aller Unternehmensdaten existieren sollten, die auf zwei verschiedenen Speichermedien gesichert sind, von denen sich wiederum eines fern des Unternehmenssitzes befindet. Erfunden hat diese Regel nicht etwa ein IT-Fachmann, sondern ein Fotograf, der selbst von einem massiven Datenverlust betroffen war. Im Jahr 2009 hat er seine daraufhin entwickelte Strategie in einem Buch veröffentlicht.

Dass seine Strategie in der Unternehmenswelt einmal zur goldenen Regel der Datensicherung aufsteigen würde, hätte er damals vermutlich nicht erwartet. Mittlerweile hat die 3-2-1-Regel aber schon sehr viele Unternehmen vor existenzbedrohenden Datenverlusten bewahrt. Aber warum genau hat sich diese Regel so durchsetzen können? Warum ist sie so wichtig?

Darum ist die 3-2-1-Regel elementar

Es gibt dafür gleich mehrere Gründe. Grund Nr. 1 haben wir Ihnen schon genannt: Ohne Daten geht es nicht. In vielen Unternehmen lässt es sich schlicht nicht mehr arbeiten, wenn der Zugriff auf Unternehmensdaten nicht möglich ist. Das bedeutet, dass der Geschäftserfolg immer stärker von einer ständigen Datenverfügbarkeit abhängt. Grund Nr. 2 lautet: Daten sind zunehmend gefährdet. Einerseits verfestigen sich die Vorhersagen, dass Klimakatastrophen wie das Hochwasser im Sommer 2021 in Zukunft häufiger werden könnten; andererseits bringen Cyberkriminelle Unternehmensdaten immer stärker in Gefahr.

Nicht minder wichtig ist Grund Nr. 3: Der Datenschutz gewinnt an Bedeutung. So ist durch die europäische Datenschutzgrundverordnung festgelegt, dass der Schutz von (personenbezogenen) Daten für jedes Unternehmen ein Muss ist. Zudem muss die Datenverfügbarkeit zu jeder Zeit gewährleistet sein. Inzwischen zeigt sich, dass die zuständigen Datenschutzbehörden bei Verstößen dagegen alles andere als zimperlich sind: Sie greifen immer härter durch und verhängen teils saftige Strafen. An einem effizienten Backup führt daher kein Weg mehr vorbei – und die 3-2-1-Regel ist diesbezüglich das Mittel der Wahl.

Dank Backup-Management sicher

Am besten holen Sie sich für die Einführung der 3-2-1-Backup-Regel Hilfe an die Seite – zum Beispiel von uns. So eine Einführung lässt sich nämlich nicht von heute auf morgen erledigen. Stattdessen gehen ihr meist einige Überlegungen voraus und es gilt einige Fragen zu klären. Auf welchen Speichermedien sollen die drei Versionen hinterlegt sein? Wie häufig sollen die Backups der Original-Daten aktualisiert werden? Wer ist dafür verantwortlich, dass die Backups zuverlässig laufen? Und wie lässt sich die 3-2-1-Regel technisch umsetzen? Antworten auf diese und weitere Fragen finden wir gern mit Ihnen gemeinsam. Lassen Sie sich in diesem Zuge am besten auch zu unserem Backup-Management beraten. Damit nehmen wir Ihnen die Durchführung und Überprüfung Ihrer Backups vollständig ab – und sorgen dafür, dass Sie sich auf Ihr Backup verlassen können!

Nutzen Sie die Firewall Mensch!

Wäre es nicht schön, wenn Cyberkriminelle mit ihren perfiden Täuschungsmanövern in Ihrem Unternehmen kontinuierlich vor die Wand fahren würden? Reines Wunschdenken ist das nicht. Immerhin gibt es ausgeklügelte technische Sicherheitsmechanismen. Und dann fehlt nur noch eines: Die Schulung der Mitarbeiter zur menschlichen Firewall!

»Schwachstelle Mensch« ist Angriffsziel

Das Cybercrime-Geschehen ist – wie bereits an anderer Stelle in dieser Ausgabe festgestellt – auf einem Allzeithoch und wird es wohl auch in den kommenden Monaten und Jahren bleiben. Das ist eine ziemlich ernüchternde Aussage, wenn man bedenkt, dass es in der Vergangenheit und Gegenwart bereits unzählige Maßnahmen gab und gibt, mit denen sich die technologischen Barrieren gegen Cyberangriffe immer höher auftürmen lassen. Grundsätzlich sind die zur Verfügung stehenden technischen Schutzmechanismen inzwischen auch so komplex und ausgefeilt, dass es sich für Angreifer immer schwieriger gestaltet, Unternehmensnetzwerke zu kompromittieren.

Das Problem ist jedoch, dass es eine ganz bestimmte Schwachstelle gibt, die sich nicht durch die Implementierung technischer Raffinessen ausbessern lässt – und genau dieser Schwachstelle wenden sich Cyberkriminelle inzwischen mit einer ganz besonderen Vorliebe zu. Es handelt sich dabei um die Mitarbeiter eines Unternehmens. Die Angreifer haben angesichts der immer ausgereifteren technischen Sicherheitsmaßnahmen mittlerweile festgestellt, dass es viel einfacher, risikoärmer und lukrativer ist, die »Schwachstelle Mensch« als Angriffsziel ins Visier zu nehmen, um sich Zugang zu Unternehmensnetzwerken zu verschaffen. Ein Blick auf die jüngere Vergangenheit zeigt, dass sich diese These längst bewahrheitet hat: Immer wieder kam es zu Sicherheitsvorfällen, bei denen Mitarbeiter das Einfallstor waren.

Phishing und Social Engineering

Mitarbeiter haben sich in der Vergangenheit also wiederholt als das schwächste Glied in der Sicherheitskette erwiesen: Laut Studien sollen etwa 95 Prozent aller Sicherheitsvorfälle in Unternehmen durch menschliches Fehlverhalten entstanden sein. Für die Angreifer scheint es daher viel einfacher zu sein, über angegriffene Mitarbeiter Zugang zu Systemen und sensiblen Informationen zu gewinnen als zum Beispiel über Schwachstellen im System. Denn: Während Sicherheitssysteme viele Netzwerke inzwischen bis in den hintersten Winkel schützen, bleibt das menschliche Verhalten an individuelle Gedanken und Gefühle sowie an persönliche Entscheidungen gebunden.

Und genau das machen sich die Angreifer zunutze, indem sie ausgefeilte Social-Engineering-Techniken zum Einsatz bringen. Das heißt: Sie wenden psychologische Tricks an, spielen dabei vor allem mit

So schulen Sie Ihre Mitarbeiter!

Mit speziellen Security-Awareness-Schulungen lässt sich sicherstellen, dass Ihre Mitarbeiter nicht auf die manipulativen Täuschungsmanöver der Cyberkriminellen hereinfallen. Dabei wird unter anderem das Sicherheitsbewusstsein aller Mitarbeiter in Bezug auf E-Mail-basierte Angriffe gestärkt. Anhand spezifischer Merkmale lernen sie, bösartige E-Mails problemlos zu erkennen. Damit der Lerneffekt noch größer ausfällt, werden Angriffe simuliert: Dadurch erlernen Mitarbeiter den kritischen Umgang mit digitalen Inhalten – und werden als menschliche Firewall trainiert. Sie haben Interesse an einer solchen Schulung? Sprechen Sie uns an!

Angst, Hoffnung, Hilfsbereitschaft, Neugierde und autoritärem Gehorsam. Ein gutes Beispiel dafür ist das Phishing. Zur Erinnerung: Mit Phishing ist gemeint, dass Cyberkriminelle versuchen, über Spam-E-Mails oder Direktnachrichten sowie über fingierte Webseiten oder Profile an persönliche Daten zu gelangen. Hierbei gelingt es ihnen immer wieder, die menschlichen Gefühle auszunutzen und ihre Opfer dazu zu verleiten, auf gefährliche Links zu klicken und Zugangsdaten einzugeben. Diese Gelegenheit wird sogleich genutzt, um die Zugangsdaten abzugreifen und für die eigenen Zwecke zu missbrauchen.

Die menschliche Firewall

Besonders spielt es den Cyberkriminellen in die Karten, wenn es ihnen gelingt, mithilfe dieser Daten ins Unternehmensnetzwerk einzudringen. Ist diese Hürde einmal überwunden, ist alles andere – ohne Netzwerksegmentierung – oft nur noch eine Fingerübung. Oft unbemerkt können sich die Angreifer im Netzwerk ausbreiten, nützliche Informationen ausspionieren und Ransomware einschleusen, um mit dieser zum geeigneten Zeitpunkt zum entscheidenden Schlag auszuholen – und dann steht im schlimmsten Fall die Unternehmensexistenz auf dem Spiel. Es versteht sich von selbst, dass Unternehmen dies unter allen Umständen verhindern sollten. Aber wie?

Indem sie die »Firewall Mensch« aktivieren. Durch spezielle Schulungen können Unternehmen ihre Mitarbeiter gezielt für die Gefahren sensibilisieren und dadurch ihre Security Awareness schulen. Das Ziel solcher Schulungen ist es, dass Mitarbeiter im Umgang mit E-Mails, Webseiten und plötzlich auftauchenden Pop-up-Fenstern besondere Vorsicht walten lassen, damit sie auf der Cybercrime-Bühne nicht ungewollt ins Rampenlicht geraten. Letztlich gilt es, sich stets die wichtigste aller Fragen zu stellen: »Klicke ich oder klicke ich nicht?«

Stück für Stück die Schotten dicht

Fakt ist: Es gibt inzwischen zahlreiche technische Schutzmaßnahmen, um Unternehmensnetzwerke so sicher wie nur möglich einzurichten und insbesondere vor Cyberangriffen zu schützen. Auch die Netzwerksegmentierung hilft dabei, das Schlimmste zu verhindern.

BSI empfiehlt sichere Netzwerkarchitektur
Die meisten Unternehmensnetzwerke werden in zunehmendem Maß komplex. Das liegt vor allem daran, dass sie neben herkömmlichen Endgeräten auch immer mehr mobile Endgeräte und Elemente, die gemeinhin dem Internet of Things (IoT) zugeordnet werden, mit einbeziehen. Hinzu kommen außerdem noch Cloud-Dienste und Kollaborationsdienste, die das Netzwerk – und damit dessen Angriffsfläche – zusätzlich vergrößern. Das Ergebnis ist, dass Cyberkriminelle immer mehr Angriffspunkte für ihre Attacken finden – und Unternehmen damit teilweise Auswirkungen mit desaströsen Ausmaßen bescheren.

Aber: Es bieten sich Unternehmen zahlreiche Möglichkeiten, um sich auch in Bezug auf die Komplexität ihres Netzwerks risikoadäquat abzusichern. Eine sinnvolle Maßnahme ist zum Beispiel die Netzwerksegmentierung, die auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem Baustein seines sogenannten IT-Grundschutz-Kompendiums thematisiert. Der Vorteil einer Netzwerkarchitektur mit einer durchdachten Segmentierung ist vor allem dieser: Dadurch, dass die einzelnen Zonen jeweils durch eine Firewall voneinander abgeschottet sind, können sich Angreifer, die es auf irgendeinem Weg in einen bestimmten Bereich des Netzwerks geschafft haben, nicht frei darin bewegen – immer wieder stoßen sie auf Mauern und können diese im Idealfall auch nicht überwinden.

Wie funktioniert die Segmentierung?
Im IT-Grundschutz-Kompendium ist festgehalten, dass ein Netzwerk mindestens in drei Zonen physisch separiert sein muss – und zwar mit einem internen Netz, einer demilitarisierten Zone (DMZ) und Außenanbindungen (zum Beispiel das Internet oder andere vertrauenswürdige Netzwerke). Die demilitarisierte Zone ist dabei über Router sowohl mit dem internen Netz als auch den Außenanbindungen verbunden – als Puffer stellt sie sozusagen die Brücke dar. Angreifer werden im Idealfall direkt in dieser Zone abgefangen und können dadurch erst gar nicht in den internen Bereich vordringen.

Dennoch kann es dazu kommen, dass es ein Eindringling schafft, diese zusätzliche Hürde zu überwinden, aus der demilitarisierten Zone auszubrechen und ins interne Netzwerk einzudringen. Und genau deshalb macht es Sinn, das interne Netzwerk noch einmal in kleinere, separate Subnetzwerke zu unterteilen, die jeweils durch eine Firewall physisch voneinander getrennt sind – die Firewall entscheidet dann auch darüber, ob ein Gerät dazu berechtigt ist, mit einem Gerät in einem anderen Netzwerksegment zu kommunizieren.

Schutzbedarf je nach Segment
Durch die Einteilung in Subnetzwerke haben Unternehmen die Möglichkeit, Sicherheitsmechanismen und Zugangskontrollen für jedes Segment individuell festzulegen. Es empfiehlt sich, Systeme mit unterschiedlichem Schutzbedarf in verschiedenen Netzwerksegmenten zu platzieren. Ist das nicht möglich, richtet sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf. Dabei ist immer sicherzustellen, dass keine Überbrückung von Netzwerksegmenten oder gar Zonen möglich ist.

Wichtig ist dabei auch: Unternehmen müssen über eine vollständige Dokumentation ihres Netzwerks verfügen und diese bei Änderungen zuverlässig pflegen. In einem Netzwerkplan sind Zonen und Subnetze genau festzuhalten. Am Ende zahlt sich die Arbeit aus. Denn: Die Netzwerksegmentierung verschafft nicht nur eine bessere Kontrolle über den Netzwerkverkehr, sondern optimiert auch die Netzwerk-Performance und den Sicherheitsstatus.

Wir sind Ihre Netzwerk-Experten!

Ein leistungsstarkes, stabiles und sicheres Unternehmensnetzwerk aufzubauen ist keine einfache Sache – und die Umsetzung einer durchdachten, korrekt dokumentierten Netzwerksegmentierung macht die Angelegenheit nicht einfacher. Grundsätzlich macht es aber für so ziemlich jedes Unternehmen Sinn, das eigene Netzwerk zu segmentieren. Besonders dann, wenn wichtige Unternehmensdaten in möglichst gut abgeschotteten Netzwerkbereichen aufbewahrt werden und vor dem Zugriff durch Unbefugte geschützt werden sollen.

Gern unterstützen wir Sie dabei, Ihr Unternehmensnetzwerk zu optimieren und setzen dabei auch die Netzwerksegmentierung inklusive Dokumentation und Netzwerkplan um. Auf Wunsch implementieren wir auch geeignete Sicherheitsmaßnahmen. Sprechen Sie uns bei Interesse einfach an!

ÜBERREICHT DURCH

DigiPhant GmbH

Nikolaus-Rüdinger-Str. 17
80999 München

Telefon +49 89 89026162
E-Mail info@digiphant.de

http://www.digiphant.de

DIGIPHANT