Wissenswertes || cebra GmbH

- Das Gesetz || 3-2-1 Regel für Backups
- Monitoring: 8 Dinge, die Sie in Ihrem Netzwerk überwachen sollten
- Als Unternehmen auf Backups verzichten? Grob fahrlässig!
- Was ist Cybersecurity?
- Verfassungsschutz warnt vor Cyberangriffen
- E-Mail-Backups sind keine rechtssichere Archivierung! 5 Irrtümer
- Passwörter im Browser speichern? Bequem! Sollten Sie aber nicht tun!
- Passwörter verwalten mit dem Passwort-Manager
- Aufgeräumt ins neue Jahr: Systeme fit für 2023

Das Gesetz || 3-2-1 Regel für Backups

cebra GmbH - new technologies Sankt Martin Str. 9, 84539 Ampfing Telefon: +49 8636 69 76 67 E-Mail: info@cebra.it Webseite: https://www.cebra.it	

Allgemeines

Autor:	Christian Sigl
Version:	2.0
Versionsdatum:	2022-07-19

Designed by macrovector from Freepik

Vorwort

Noch mal "schnell" die E-Mails checken - ein falscher Klick - und es ist zu spät - ihre Daten sind verschlüsselt oder gelöscht! Leider ist dieses Horrorszenario immer wieder Thema in vielen Unternehmen, weshalb wir uns heute dem Thema Datensicherungskonzept widmen werden.

Die 3-2-1-Regel für Datensicherungen gilt für den Großteil der Techniker in der IT-Welt als Gesetz. Sie soll sicherstellen, dass durch ein geeignetes Datensicherungskonzept keine Unternehmensdaten verloren gehen. Wie wichtig das Thema ist und warum es von den Unternehmen sehr ernst genommen werden sollte erfahren Sie im folgenden Artikel.

Kein Backup? Kein Mitleid!

Ihre Daten sind nicht nur durch einen Verschlüsselungstrojaner oder Virus gefährdet. Daten werden unachtsam gelöscht - Speichermedien versagen - ein Kurzschluss macht die Hardware unbrauchbar - ein Feuer im Gebäude könnte die gesamte IT-Infrastruktur zerstören - sämtliche Daten könnten durch einen Hackerangriff gelöscht werden.

Designed by www.slon.pics from Freepik

Sind die Daten erstmal weg, ist der Schaden unter Umständen enorm. Stellen Sie sich vor Sie verlieren als Unternehmen Ihre Kundendaten, E-Mails und Termine. Vielleicht auch Bestellungen, Rechnungen, Personalunterlagen oder gar Projektzeichnungen in die viel Zeit investiert wurde. Für viele Unternehmen kostet das nicht nur Zeit und Geld, sondern in gravierenden Fällen sogar die Existenz des Unternehmens.

Wie schön wäre es, wenn man die Unternehmensdaten im Fall der Fälle ganz einfach wiederherstellen könnte?

Mit der richtigen Backupstrategie ist das kein Problem! Schreiben Sie sich die goldene 3-2-1 Regel am besten besonders dick hinter die Ohren und verlieren Sie keine Zeit mit der Implementierung!

Was genau bedeutet die 3-2-1 Regel?

Wie im Vorwort bereits erwähnt gilt die 3-2-1 Regel unter Technikern als Gesetz der Datensicherheit. Im Grunde erscheint das Thema vorerst komplizierter als es eigentlich ist.

Es sollen **drei** Kopien oder Versionen aller Unternehmensdaten existieren. Hier handelt es sich zum einen um die Original-Daten (auch Primärdaten), welche produktiv in der täglichen Arbeit genutzt werden und zum anderen um zwei Kopien, welche als Backup dienen.

Die Wahrscheinlichkeit, dass auf drei Geräten gleichzeitig etwas schief geht, ist natürlich sehr viel geringer. **Zwei** der gesicherten Versionen sollten sich auf verschiedenen Speichermedien befinden, wobei sich **eine** Sicherung fern des Unternehmenssitzes befinden sollte.

Sollte eines der Medien einen Defekt aufweisen, wären immerhin noch zwei weitere Kopien der Unternehmensdaten vorhanden sodass die Daten ohne Weiteres wiederhergestellt werden können.

Gehen Sie bei diesem Thema immer von Murphys Gesetz aus, weshalb wir uns im folgendenen der Risikominimierung widmen.

> “Anything that can go wrong *will* go wrong.”
>
> "Alles, was schiefgehen kann, wird auch schiefgehen"
>
> Murphys Gesetz

Risikominimierung

Mit jeder Backupkopie sinkt das Risiko eines kompletten Datenverlustes enorm. Warum also eine Sicherung nicht ausreicht, lässt sich anhand statistischer Ausfallwahrscheinlichkeiten leicht beantworten.

Sobald die Primärdaten und deren Kopien auf zwei unterschiedlichen Systemen mit gleichen Eigenschaften aufbewahrt werden liegt die Ausfallwahrscheinlichkeit bei 1:10.000.

Dies ist durch die Tatsache gegeben, dass die Wahrscheinlichkeit, dass diese Medien aus unterschiedlichen Gründen und damit unabhängig voneinander ausfallen, jeweils 1:100 beträgt.

Die daraus resultierende Berechnung ergibt sich also zu 1/100 * 1/100 = 1/10.000.

Fügt man dieser Berechnung eine weitere Datensicherung auf einem dritten unabhängigen System hinzu nimmt die Wahrscheinlichkeit eines gleichzeitigen Ausfalls aller drei Geräte auf 1/1.000.000 ab.

Warum ist der "Medienbruch" bei der 3-2-1 Regel so entscheidend?

Liegen Primärdaten und Datensicherungen an demselben Speicherort, können sie auch von demselben technischen Fehler betroffen sein. Fällt zum Beispiel eine Festplatte aus, kann es

durchaus vorkommen, das kurze Zeit später eine weitere Festplatte desselben Storagesystems ausfällt.

Es geht letztendlich um den Einsatz verschiedener Speichertechnologien mit unterschiedlichen Eigenschaften und Ausfallwahrscheinlichkeiten und der Kombination aus Diesen, um das Risiko eines kompletten Datenverlustes verringern zu können.

Externer Aufbewahrungsort im Worst-Case-Szenario

Die "1" in der 3-2-1-Regel beschreibt den externen Aufbewahrungsort der dritten Version der Primärdaten. Extern bedeutet in dem Zusammenhang nicht nur ein anderes Gebäude, sondern fern vom Unternehmensstandort.

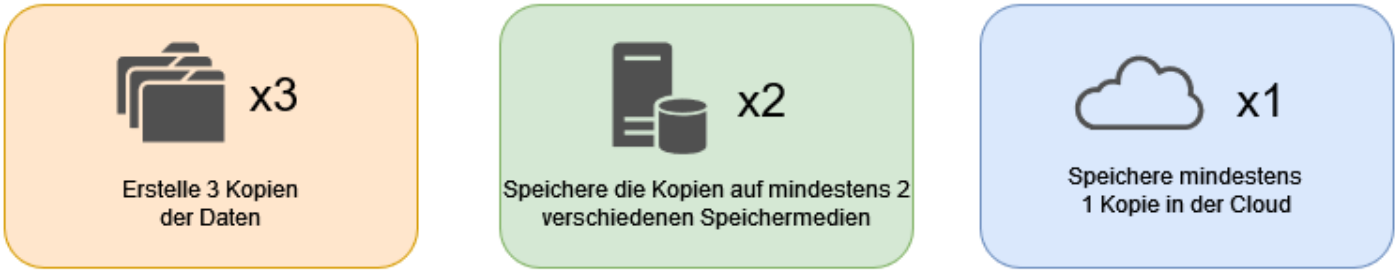
Designed by Freepik from Freepik

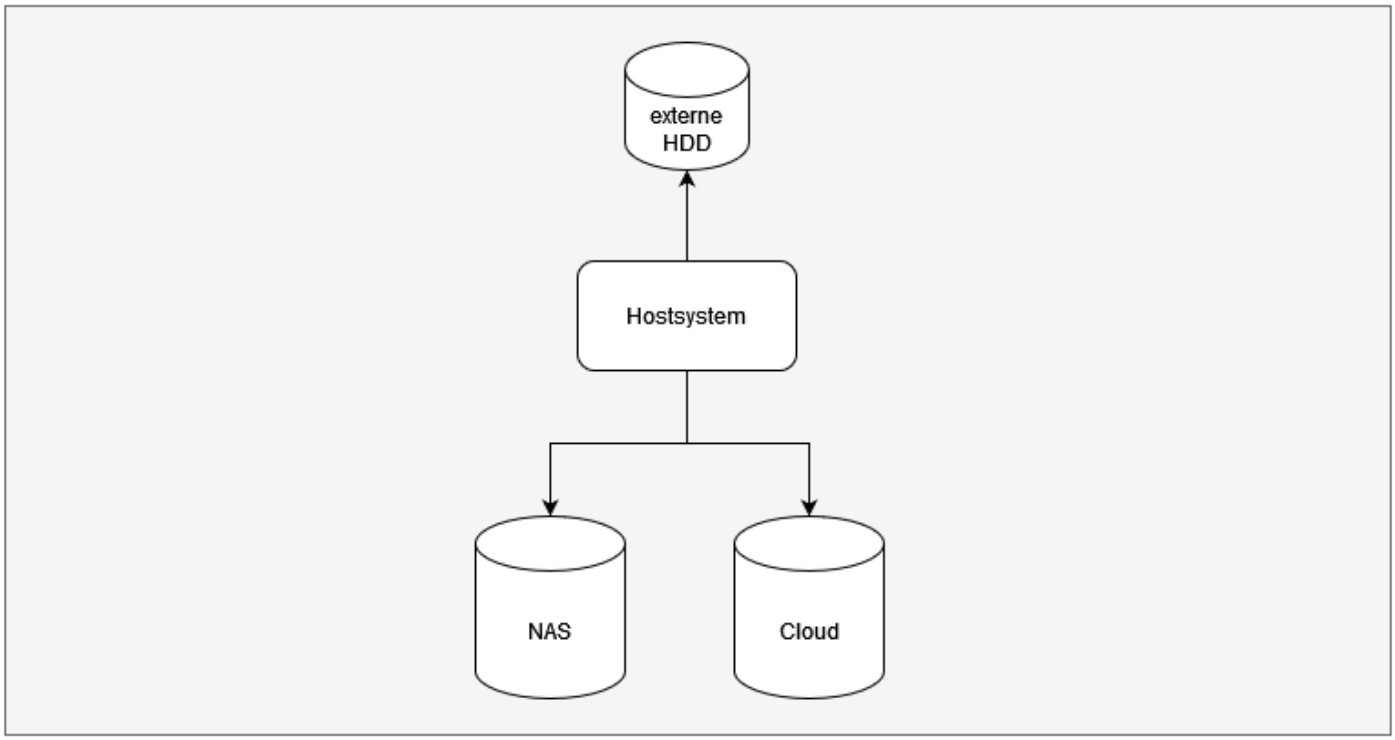
Die resultierende Notwendigkeit ergibt sich aus der Gefahr von äußeren Einflüssen wie Hochwasser, Brand oder einem Kurzschluss. In solchen Fällen sind die Datensicherungen am Firmenstandort - auch wenn eine, zwei oder drei Kopien existieren - wertlos.

Nur so lässt sich sicherstellen, dass alle Ihre Unternehmensdaten im Worst-Case-Szenario wiederhergestellt werden können.

Backupkonzept

Zu guter Letzt möchte ich Ihnen die Strategie noch visuell veranschaulichen und Ihnen damit ein geeignetes Konzept für Ihr Unternehmen an die Hand geben.





Monitoring: 8 Dinge, die Sie in Ihrem Netzwerk überwachen sollten

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	3.0
Versionsdatum:	2022-08-02

Vorwort

> **Handeln Sie proaktiv und nicht reaktiv - ihr Geldbeutel wird es Ihnen früher oder später danken!**

Eine konsequente Überwachung aller Server, Rechner und Netzwerkgeräte kann Ihnen enorm viel Zeit und vor allem Nerven sparen. Mit geeigneten Monitoring Tools können Sie mögliche Fehler frühzeitig erkennen und anschließend proaktiv beheben. Was man überprüfen sollte und wann ein Eingreifen erforderlich ist erfahren Sie im folgenden Artikel.

Designed by rawpixel.com from Freepik

1. Performance

Mithilfe geeigneter Tools können Sie prüfen, ob Ihre Systeme beeinträchtigt oder optimierbar sind. Es kann z.B. die Festplattenaktivität, Speicher- oder CPU-Auslastung in Echtzeit überwacht und so Rückschlüsse auf Performanceengpässe gemacht werden. Liegt die aktive Datenträgerauslastung für einen bestimmten Zeitraum (z.B. 10 Minuten) über einen definierten Schwellwert von z.B. 90%, sollte die Ursache geprüft werden.

2. Potentielle Festplattenfehler

Mithilfe der Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T) können Festplattenlaufwerke (HDD) und Solid-State-Drives (SSD) überwacht und so Vorhersagen eines möglichen Ausfalls getroffen werden. Verschlechtert sich zum Beispiel die Anzahl der brauchbaren Sektoren einer Festplatte, sollte man sich langsam Gedanken um einen Austausch der HDD machen, um einen Ausfall des Gesamtsystems zu vermeiden.

3. Kapazitätsgrenze Festplattenspeicher

Immer wieder kommt es vor, dass die internen Festplatten eines Systems durch Software, Logfiles, temporäre Updatedateien und Backupdaten vollgeschrieben werden. Erreicht der freie Speicherplatz einen kritischen Schwellwert von beispielsweise 10-15%, kann automatisiert eine Festplattenbereinigung mit dem Löschen temporärer Dateien gestartet werden.

4. Ausstehender Neustart von Geräten

Server, Workstations und Mobile Clients wie Notebooks sollten in regelmäßigen Abständen neu gestartet werden. Nach der Installation von Windows Updates oder wichtigen Sicherheitspatches erfordern die Systeme meist einen Neustart um die Installationen abschließen zu können.

5. Ausführung kritischer Anwendungen

Fallen kritische Anwendungen oder Dienste auf einem Server aus, können diese in Echtzeit identifiziert und unmittelbar neu gestartet werden. In den meisten Fällen ist die Ausfallzeit eines Dienstes mit einem geeigneten Monitoring-Tool so gering, dass die Mehrheit der Mitarbeiter den Ausfall gar nicht mitbekommt.

6. Netzwerküberwachung

Mit einer Monitoring-Software können Sie außerdem prüfen, ob alle notwendigen Netzwerkgeräte verfügbar sind sowie offene Ports oder die Verfügbarkeit von Kunden-Websites überwachen. Wird z.B. aus irgend einem Grund die Windows-Firewall deaktiviert (z.B. durch einen unerlaubten Zugriff), besteht die Möglichkeit sich automatisch benachrichtigen zu lassen und die Windows-Firewall wieder zu aktivieren.

7. Fehlerhafte Anmeldeversuche von Benutzern

Über einen Windows-Fehler im Ereignisprotokoll lässt sich nachvollziehen, ob ein Benutzer versucht hat, sich mit einem falschen Passwort anzumelden. Bei Überschreitung einer bestimmten Anzahl an Anmeldeversuchen können Sie sich umgehend benachrichtigen lassen und anschließend der Ursache auf den Grund gehen.

8. Fehlgeschlagene Backups

Eines der wichtigsten Themen ist wohl das Thema Datensicherung. Für nähere Informationen möchte ich Sie auf den Artikel **Das Gesetz || 3-2-1 Regel für Backups** verweisen. Hier finden Sie alle wichtigen Informationen rund um das Thema Datensicherung.

Mithilfe einer Monitoring-Software können Sie sich natürlich auch im Falle von fehlerhaften Backups benachrichtigen lassen. So können Sie schnellstmöglich reagieren, sodass Sie im Worst-Case-Szenario alle Daten wiederherstellen können.

Fazit

Ein effektives Monitoring kann Ihnen unter Umständen enorm viel Zeit, Geld und Nerven sparen. Sie als Geschäftsführer(in) müssen letztendlich die Kosten für einen Ausfall der IT-Infrastruktur tragen. Aus diesem Grund sollten Sie unbedingt tätig werden und eine geeignete Monitoring-Lösung implementieren.

Mit diesen hilfreichen Tools können Sie nicht nur interne Hardwarekomponenten wie die CPU oder die Festplatten eines Systems überwachen, sondern auch die Systeme von temporären Altdaten bereinigen und automatisierte Neustarts durchführen.

> **Handeln Sie proaktiv und nicht reaktiv**!

Als Unternehmen auf Backups verzichten? Grob fahrlässig!

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2022-09-07

Designed by www.slon.pics from Freepik

Vorwort

Daten sind das Gold des 21. Jahrhunderts! Das wird Ihnen nicht nur jeder ITler bestätigen - auch Unternehmen, welche schon einen oder mehrere Datenverluste zu verzeichnen haben, wissen wie kostbar die Datenbestände sind.

Gerade aus diesem Grund sind Ihre Daten immer vielfältigeren Bedrohungen ausgesetzt! Bedrohungen lauern aber nicht nur von externen Angreifern, sondern sind auch des Öfteren den eigenen Mitarbeitern geschuldet. Hier erfahren Sie, welche die gängigsten Gefahren für Ihre Daten sind. Im Anschluss werden Sie erkennen, wie wichtig moderne Backup-Strategien sind.

Bedrohungen

1. Unwissenheit und Ignoranz
Sie werden sich denken: "Dann muss man sich halt informieren." Und genau das ist der entscheidende Punkt! Wenn die Entscheider die Notwendigkeit moderner Backup-Strategien nicht erkennen, nicht erkennen wollen oder das Thema aufgrund vor der Angst hoher Kosten meiden, sind Geschäftsdaten permanent in Gefahr. Jedes Unternehmen wird früher oder später einen

Datenverlust verzeichnen - die Frage ist nur, in welchem Ausmaß.

2. Veraltete Software
Ein fehlendes regelmäßiges Patch-Managment erhöht das Risiko von Datenverlust enorm. Dabei sollte nicht nur das Betriebssystem, sondern auch die auf dem System installierte Software regelmäßig aktualisiert werden. Werden Systeme nicht kontinuierlich mit den neuesten Updates versorgt, steigt damit auch die Gefahr eines Softwarefehlers oder Ausfalls. Zudem ist eine veraltete Software ein gefundenes Fressen für Hackerangriffe.

3. Menschliches Versagen
Ich denke jeder kennt das Szenario: Spät am Nachmittag - die Konzentration schwindet und schwub hat man aus Versehen eine falsche Datei gelöscht. Mit einer durchdachten Backup-Strategie sichern Sie sich gegen solche Vorfälle ab.

4. Vorsätzliche Löschung
Leider muss man sagen, dass dieses Szenario auch durch mutwillige Zerstörung von Daten existiert. Es kommt immer wieder vor, dass sich entlassene Mitarbeiter am Unternehmen rächen wollen und kurzer Hand alle Daten löschen auf die sie Zugriff haben. Nicht nur deshalb sollte man allen Mitarbeitern auch nur Zugriff auf Daten freischalten mit denen sie tatsächlich auch arbeiten müssen.

5. Datendiebstahl
Daten können genau wie physische Gegenstände entwendet werden. Es muss sich hier nicht einmal um einen Hackerangriff oder einen abtrünnigen Mitarbeiter handeln, welcher vertrauliche Informationen zur Konkurenz mitnimmt - auch eine verlorene oder gestohlene externe Festplatte bzw. ein USB-Stick können einen Datenverlust zufolge haben.

6. Ransomware
Ransomware sind Schadprogramme, welche Daten auf einem Computer verschlüsseln. Die Täter erpressen ihre Opfer anschließend mit einer Lösegeldzahlung um die verschlüsselten Daten wieder freizugeben. Diese Form der Cyberkriminalität wächst weiterhin drastisch - Tendenz steigend. Eine globale Studie zeigt, dass alleine in Deutschland knapp 69% der Unternehmen schon von einem Ransomware-Angriff betroffen waren.

7. Hackerangriffe, Trojaner und Viren
Neben der oben genannten Ransomware gibt es natürlich noch zahlreiche andere Trojaner, Würmer oder Viren, die Ihre IT-Infrastruktur zum Erliegen bringen können. Auch hier empfiehlt sich, nicht darauf zu hoffen, dass Sie verschont bleiben.

8. Technisches Versagen
Neben den menschlichen Gefahren, darf man auch technische Fehler nicht außer Acht lassen! Es kann immer wieder vorkommen, dass Festplatten oder gar ihr gesamter Server ausfällt. Mit einer geeigneten Backup-Strategie, mit unterschiedlichen Speicherorten und -medien, verhindern Sie den Verlust Ihrer geschäftskritischen Daten.

9. Fehlerhafte Backup-Strategien
Auch wenn Ihre Daten gesichert werden, garantiert das noch lange nicht die Verfügbarkeit im Ernstfall. Auch ein Backup kann fehlerhaft sein, vorloren gehen oder unvollständig sein. In der Praxis hat sich daher die 3-2-1-Regel durchgesetzt: Erstellen Sie *drei* Kopien auf *zwei* unterschiedlichen Speichermedienarten und lagern Sie mindestens *eines* davon an einem externen Speicherort.

10. Elementargewalten
Viele Unternehmer schenken dieser Gefahr keinerlei Beachtung, da die Wahrscheinlichkeit einer Naturkatastrophe zugegebenermaßen vergleichsweise gering zu den oben genannten Punkten ist. Aber glauben Sie mir: Es kommt vor! Sie dürfen auch nicht außer Acht lassen, dass Ihre Daten und Datensicherungen durch Brände, Überschwemmungen und Sturmschäden zerstört werden könnten. Dies muss auch nicht zwangsläufig in Ihrem Unternehmen geschehen - auch große Rechenzentren können davon betroffen sein (Am Rhein brennt Europas Datenschatz). Umso wichtiger ist es, mehrere verschiedene Backupziele zu nutzen.

Fazit

Seien Sie nicht naiv! Es stellt sich nicht die Frage ob ein Unternehmen von einem Datenverlust betroffen sein wird - die Frage lautet wann und in welchem Ausmaß wird der Datenverlust sein. Schützen Sie sich vor diesen Bedrohungen! Sichern Sie Ihre Server, Workstations und auch Cloud-Daten nach dem Großvater-Vater-Sohn-Prinzip und beachten Sie dabei die 3-2-1-Regel. Sprechen Sie uns an - wir beraten Sie gerne.

Was ist Cybersecurity?

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	4.0
Versionsdatum:	2022-12-19

Vorwort

"Es gibt nur zwei Arten von Unternehmen: Solche, die gehackt wurden, und solche, die noch gehackt werden." Robert Mueller, ehem. FBI-Chef, 2012, zit. im "Rechtshandbuch Cyber-Sicherheit", Gabel/Heinrich/Kiefer (Hrsg.), 2019.

Ich würde derzeit sogar noch einen Schritt weitergehen und das Zitat erweitern um **"solche, die gehackt wurden, es aber noch nicht wissen."**

Leider können wir derzeit täglich mehrere Cyber-Angriffe auf kleine und mittelständische Unternehmen verzeichnen - Tendenz steigend. Dabei ist nicht immer klar, welches Ziel die Angreifer verfolgen. In manchen Fällen geht es nur darum im Unternehmen Schaden anzurichten. Oftmals werden die Firmen aber auch mit einer Lösegeldforderung konfrontiert, um an die heiligen Unternehmensdaten wieder heranzukommen.

Ein **ganzheitliches** Sicherheitskonzept ist deshalb unumgänglich - auch für den Mittelstand!

Stellen Sie sich Ihr Netzwerk als Ihr eigenes Zuhause vor. Hier werden Sie sich vermutlich auch schützen indem Sie alle Türen und Fenster schließen. Sie können noch so ein hochmodernes Sicherheitsschloss an Ihrer Haustür besitzen - wenn Sie das Fenster offen lassen kommt der Eindringling in Ihr Haus.

Genauso ist es auch mit Ihrem Unternehmensnetzwerk. Es nützt relativ wenig nur eine Tür gut zu sichern - der Angreifer wird früher oder später das offene Fenster finden.

Was ist also Cybersecurity?

Unter Cybersicherheit versteht man Maßnahmen, um Computer, Server, Mobilgeräte, elektronische Systeme, Netzwerke und Daten gegen böswillige Angriffe zu verteidigen. Sie wird auch als IT-Sicherheit oder elektronische Datensicherheit bezeichnet. Der Begriff wird in einer Vielzahl von Kontexten, von Geschäftsanwendungen bis zum mobilen Computing, verwendet und lässt sich in einer Reihe von allgemeinen Kategorien zusammenfassen.

- **Netzwerksicherheit** ist ein Verfahren zur Sicherung eines Computernetzwerkes vor Eindringlingen, sei es in Form von gezielten Angreifern oder einer auf eine günstige Gelegenheit hoffenden Malware.
- **Programmsicherheit** bezieht sich darauf, Software und Geräte von Bedrohungen zu bewahren. Ein gefährdetes Programm könnte Zugriff auf die Daten gewähren, die es eigentlich schützen soll. Erfolgreiche Sicherheit beginnt in der Designphase, noch lange bevor ein Programm oder Gerät bereitgestellt wird.
- **Informationssicherheit** schützt die Integrität und Privatsphäre von Daten, sowohl in Speichern als auch beim Versenden.
- **Betriebssicherheit** bezieht sich auf Prozesse und Entscheidungen zum Umgang und Schutz von Datenbeständen. Unter diese Bezeichnung fallen die Berechtigungen, über die ein Benutzer beim Zugriff auf ein Netzwerk verfügt, sowie die Verfahren, über die festgelegt ist, wie und wo Daten gespeichert oder freigegeben werden dürfen.
- **Disaster Recovery und Business Continuity** definieren, wie eine Organisation auf eine Verletzung der Cybersicherheit oder jedes andere Ereignis, das zum Verlust betrieblicher Abläufe oder Daten führen, reagieren. Wie eine Organisation ihren Betrieb und ihre Daten auf denselben Stand wie vor dem Ereignis wiederherstellt, ist in den Disaster Recovery-Richtlinien festgelegt. Auf den Business Continuity-Plan greifen Organisationen zurück, um die eigene Geschäftstätigkeit auch ohne bestimmte Ressourcen fortsetzen zu können.
- Bei der **Endbenutzer-Aufklärung** geht es um den am wenigsten vorhersagbaren Faktor der Cybersicherheit: den Menschen. Jeder kann versehentlich ein Virus in ein ansonsten sicheres System einschleusen, indem er bewährte Sicherheitsprinzipien verletzt. Benutzer darüber aufzuklären, dass verdächtige E-Mail-Anhänge gelöscht oder unbekannte USB-Sticks nicht eingesteckt werden dürfen, sowie eine Reihe von weiteren wichtigen Lektionen sind für die Sicherheit jeder Organisation unverzichtbar.

Katz-und-Maus-Spiel

Die kontinuierliche Entwicklung

Eine der größten Herausforderungen im Bereich Cybersecurity ist die stetige Weiterentwicklung der Technologien. Neue Technologien bieten auch neue potenzielle Möglichkeiten und Angriffspunkte für Cyberkriminelle. Im Umkehrschluss heißt dies, dass auch die Security Software Anbieter und Sicherheitsexperten ständig neue Lösungen zur Schließung von Schwachstellen entwickeln müssen.

Klar - eine sehr große Herausforderung für kleine und mittelständische Unternehmen - zumal der Ganze Spaß nicht nur nervenaufreibend sondern auch sehr kostenspielig werden kann, da die Sicherheit immer mit dem Komfort und der Bequemlichkeit einhergeht und die Systeme ständige Aufmerksamkeit und regelmäßige Updates benötigen, um potentielle Sicherheitslücken schnellstmöglich zu schließen.

Ausbildung der Mitarbeiter

Die Angriffszenarien haben sich in den letzten Jahren stark verändert. Dabei war es vor nicht allzulanger Zeit üblich, Systeme etwa mit einer Brute-Force-Attacke anzugreifen. Aufgrund zusätzlicher Sicherheitsmechanismen, wie zum Beispiel einer Multi-Factor-Authentifizierung (MFA), ist dies für Angreifer oft nicht mehr das richtige Werkzeug, weshalb mehr und mehr auf den Faktor Mensch, mithilfe Social Engineering, gesetzt wird.

Fazit

Seien Sie nicht naiv! Schützen Sie Ihr Unternehmensentzwerk mithilfe geeigneter Maßnahmen, sensibilisieren Sie Ihre Mitarbeiter und handeln Sie proaktiv. Wir sind in einem digitalen Zeitalter angekommen, bei dem sich nicht die Frage stellt ob Ihr Unternehmen angegriffen wird. Es wird passieren! Vielmehr sollten Sie sich die Frage stellen, ob Sie gegen aktuelle Angriffe bestmöglich geschützt sind, um das Ausmaß der Angriffe auf ein Minimum reduzieren zu können.

Sprechen Sie uns an - wir beraten Sie gerne.

Verfassungsschutz warnt vor Cyberangriffen

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	2.0
Versionsdatum:	2022-09-15

Sicherheitshinweise

2022-03-04-Sicherheitshinweis.pdf

Bedrohungslage

Die Bedrohungslage im Bereich von Cyberangriffen hat sich auch durch den Krieg in der Ukraine extrem verschärft. Die Lage um die Sicherheit in der Informationstechnik ist ernst. Aus diesem Grund hat der Verfassungsschutz Sicherheitshinweise veröffentlicht. Es besteht ein erhöhtes Risiko von Cyberangriffen gegen deutsche Einrichtungen und besonders auch gegen Unternehmen. Sie sollten die Entwicklungen aufmerksam beobachten und Ihre IT-Sicherheitsmaßnahmen entsprechend anpassen. Mehrere Schadprogramme (zum Beispiel WhisperGate, HermeticWiper) machen Geräte funktionsuntüchtig oder werden zur Manipulation von Daten verwendet.

Da die benannte Wiper-Malware nur kurze Zeit benötigt, um ein System zu zerstören, ist Prävention besonders wichtig – jeder kann betroffen sein.

Das Bundesamt für Verfassungsschutz gibt folgende Handlungsempfehlungen:

- Weil der Angreifer für das Platzieren und die Ausführung der Malware eine Zugriffsmöglichkeit auf das System besitzen muss, ist es dringend empfehlenswert, mögliche Angriffsvektoren zu minimieren. Es ist sorgfältig zu überlegen, welche Vorgänge und Systeme aktuell für die Gewährleistung der Funktionalitäten eines Unternehmens unbedingt erforderlich sind.

- Backups müssen in regelmäßigen Abständen angefertigt und anschließend von den betroffenen Systemen getrennt aufbewahrt werden.

- Bekannte Sicherheitslücken müssen durch das Einspielen vorhandener Update-Patches geschlossen werden und sind somit als Angriffsvektor verschlossen.

- Intrusion Detection Management Systeme (IDMS) sollten in der Lage sein, die Malware zu erkennen und zu blockieren. Dafür muss aber dem IDMS die Berechtigung gegeben werden, das Starten und Ausführen entsprechender Prozesse nicht nur zu protokollieren, sondern diese auch sofort zu stoppen und Dateien in Quarantäne verschieben zu können.

- Unbekannte oder nicht mehr verwendete Nutzer müssen entfernt und Berechtigungen für Nutzer auf ein Minimum reduziert werden.

- Zum Schutz vor (Credential-)Phishing-Angriffen müssen Konten nach Möglichkeit mit Multi-Faktor-Authentifizierung geschützt werden.

- Misstrauen Sie allen E-Mails, die Sie zu dringenden Handlungen auffordern. Geben Sie niemals Ihre Passwörter an und klicken Sie niemals auf Links oder Anhänge verdächtiger E-Mails. Dies gilt auch für E-Mails von Familie, Freunden oder dem Arbeitgeber. Deren E-Mail-Konten könnten ebenfalls gehackt worden sein.

- Die aktuelle Bedrohungslage muss den Mitarbeiterinnen und Mitarbeitern bekannt gemacht werden, um ein Gefährdungsbewusstsein zu schaffen.

- Etablierung und Bekanntmachung von Meldeprozessen bei Auffälligkeiten und Sicherheitsvorfällen innerhalb des Unternehmens sowie der Ansprechbarkeiten von Behörden.

Den kompletten Sicherheitshinweis des Bundesamtes für Verfassungssicherheit finden Sie im Anhang. Hier sind auch Kontaktdaten für Meldungen oder Rückfragen aufgeführt.

Nehmen Sie diesen Hinweis bitte sehr ernst und treffen Sie entsprechende Vorkehrungen.

E-Mail-Backups sind keine rechtssichere Archivierung! 5 Irrtümer

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2022-12-19

Vorwort

„Backups und E-Mail-Archivierung sind das Gleiche“

„E-Mail-Archivierung gilt nur für Konzerne“

"Ich drucke ja alle meine E-Mails aus"

Diese Aussagen hören wir fast täglich in Kundengesprächen.

Diese gängigen Irrtümer können allerdings schwerwiegende rechtliche Folgen für Unternehmen haben – vor allem, wenn durch E-Mails ein Geschäft vorbereitet, abgeschlossen, abgewickelt oder

rückgängig gemacht wurde (z. B. Rechnungen, Angebote, Support- oder Terminanfragen).

Hier die größten 5 Irrtümer, die vor allem in kleinen und mittelständischen Unternehmen weit verbreitet sind:

1. "E-Mail-Archivierung gilt nur für Konzerne"

Jeder Geschäftsbetrieb, egal welcher Größe, ist verpflichtet, E-Mails ordnungsgemäß aufzubewahren. Denn: Alle Unternehmen mit einer Gewinnerzielungsabsicht unterliegen den Prinzipien der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern (GoBD).

Bedeutet: Jedes Unternehmen muss E-Mails archivieren!

2. "Backups und E-Mail-Archivierung sind das Gleiche"

Ein Backup wird in der Regel täglich zu einem bestimmten Zeitpunkt erstellt und bildet eine Momentaufnahme des Systems ab. Gelöschte oder geänderte Dateien werden dabei nach einer gewissen Zeit überschrieben. Diese Form der Datensicherung ist nicht manipulationssicher und reicht daher nicht aus, um eine revisionssichere E-Mail-Archivierung zu gewährleisten. Hier benötigt es zwingend eine E-Mail-Archivierungslösung, wie die unseres deutschen Herstellers MailStore, welche unter anderem durch Journalarchivierung für ein „komplettes Archiv“ sorgt.

3. "Der Datenschutz verbietet eine E-Mail-Archivierung"

Datenschutz und E-Mail-Archivierung lassen sich mithilfe regelbasierter Löschung in Einklang bringen. Dabei wird festgelegt, dass Nachrichten mit personenbezogenen Daten – beispielsweise Bewerbungsunterlagen mit u. a. dem Vor- und Nachnamen einer Person – nach den gesetzlichen Fristen automatisiert gelöscht werden. Wie dies DSGVO-konform mit der E-Mail-Archivierungslösung von MailStore umgesetzt werden kann, erfahren Sie bei der cebra GmbH.

4. "E-Mails ausdrucken und abzulegen, ist ausreichend"

Nach den GoBD dürfen nur Belege im Originalformat zur Aufbewahrung geschäftlicher Dokumente genutzt werden. Die E-Mail als digitales Dokument muss also zwingend auch digital archiviert werden, da nur so das Originalformat erhalten bleibt. Der Ausdruck einer Mail gilt als Kopie und würde im Rahmen der Beweislastsicherung vor Gericht beispielsweise nicht standhalten.

5. "Nur Rechnungen müssen archiviert werden"

Unternehmen sind laut § 257 HGB / §140 AO verpflichtet, den gesamten Geschäftsprozess zu archivieren – also Rechnungen sowie alle anderen geschäftsrelevanten Nachrichten, beispielsweise Angebotsanfragen, Rücksprachen rund um Projekte, Auftragserteilungen und Lieferbelege.

Fazit

Eine E-Mail-Archivierung und ein E-Mail-Backup können durchaus Gemeinsamkeiten haben, verfolgen aber unterschiedliche Ziele. Das Ziel jeder E-Mail-Archivierung sind in erster Linie die Revisionssicherheit und eine Wiederauffindbarkeit sowie dauerhafte Verfügbarkeit von E-Mail-Daten (Text und Anhang). Ein Backup hingegen gewährleistet eine kurz- bis mittelfristige und regelmäßige Speicherung von Daten und stellt eine Momentaufnahme der gesicherten Daten dar. Es braucht also Beides! Tiefergehende Informationen zu den verschiedenen Zielsetzungen finden Sie in unserer ausführlichen Gegenüberstellung.

E-Mail-Archivierung-Gegenüberstellung.pdf

E-Mail-Archivierung-Gegenüberstellung.docx

Passwörter im Browser speichern? Bequem! Sollten Sie aber nicht tun!

cebra GmbH - new technologies Sankt Martin Str. 9, 84539 Ampfing Telefon: +49 8636 69 76 67 E-Mail: info@cebra.it Webseite: https://www.cebra.it	

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2022-12-22

Vorwort

Wer kennt es nicht? Passwort für eine Website (z.B. Facebook, Dropbox etc.) im Browser eingeben - man wird gefragt, ob man das Passwort im Browser speichern möchte - super! Dann muss ich es beim nächsten Login nicht erneut eintippen.

Sehr bequem, aber gefährlich!

Anmeldeinformationen stehen im Fokus von Angreifern und werden sogar im Darknet gehandelt!

Das Erschreckende: Anmeldeinformationen, welche am PC z.B. in einer Remotesitzung oder im Webbrowser hinterlegt wurden, lassen sich innerhalb weniger Minuten und

ohne große Vorkenntnisse auslesen!

Wenn Hacker Netzwerke und Active Directory angreifen, verwenden sie gerne die immergleichen Tools und Vorgehensweisen. In den meisten Fällen „hacken“ Angreifer auch nichts, sondern sie erhalten über verschiedene Wege, zum Beispiel durch Social Engineering, die Anmeldedaten eines Benutzers. Mit denen melden sich die Hacker dann ganz normal an.

Cyberattacken basieren meistens auf dem Diebstahl von Identitäten und Anmeldeinformationen. Hinzu kommt, dass in nahezu allen Organisationen Endgeräte existieren, auf denen Anmeldeinformationen nicht ausreichend geschützt sind, zum Beispiel zwischengespeicherte Anmeldeinformationen für die Remoteeinwahl oder Login-Daten in Webbrowsern. Die recht prominente WannaCry-Ransomware ist zum Beispiel bekannt dafür, RDP-Sitzungen zu kapern.

Hacker hacken nichts, sie melden sich einfach an

Hacker hacken also meistens nicht, sie melden sich einfach mit ergaunerten Anmeldedaten an. Erst anschließend beginnt die eigentliche Aktivität des Angreifers. Wenn er sich erfolgreich im Netzwerk positioniert hat, versucht er, an weitere Anmeldedaten zu kommen, die er mit Tools wie LaZagne, BloodHound und Mimikatz in lokalen Netzwerken abgreift. Dabei hat er immer Konten mit einer höheren Berechtigungsstufe im Fokus, bis schlussendlich auch Anmeldedaten oder Kerberostickets von Administratoren oder anderen privilegierten Konten in Active Directory vorliegen.

Die bekannte Hackerin Alissa Knight sagt dazu: „Sobald ich in einem Netzwerk eine Lücke gefunden habe, mache ich mich zunächst auf die Suche nach Domänenadministrator-Rechten, indem ich Anmeldeinformationen aus dem Speicher der Systeme auslese. Ich suche so lange, bis ich solche Rechte in einem Netzwerk finde. Und das tue ich immer!“.

Handelt es sich bei dem gekaperten Konto um ein privilegiertes Benutzerkonto, sind die Schutzfunktionen in den meisten Unternehmen bereits ausgehebelt, bevor irgendjemand etwas von dem Angriff bemerkt.

Passwörter verwalten mit dem Passwort-Manager

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2023-01-04

Vorwort

Sichere Passwörter für alle Onlinekonten sind essenziell. "123456", "hallo" und "Passwort" zählen immer noch zu den am häufigsten vorkommenden Passwort-Kombinationen. Ein Passwort-Manager hilft dabei, verschiedene, komplexe Passwörter zu verwalten.

Die Wichtigsten Informationen rund um Passwort-Manager finden Sie im Folgenden.

Lohnt sich ein Passwort-Manager?

Ja, in der Regel lohnt sich der Einsatz eines Passwort-Managers. Es ist in jedem Fall besser, als gängige Passwörter wiederholt zu benutzen. Die konkrete Entscheidung darüber, welches Programm genutzt wird, erfordert ein individuelles Abwägen der jeweiligen Nutzung. Es geht dabei auch um die Einschätzung des damit verbundenen Risikos.

Wie funktioniert ein Passwort-Manager?

Für einige ist es deswegen eine Strategie, sich ein besonders komplexes Passwort für alle Accounts zu merken. Doch ist dieses einmal geknackt, können Cyber-Kriminelle auf alle sensiblen Daten zugreifen. Am sichersten ist es aus diesem Grund, für jeden Account ein eigenes, komplexes Passwort zu haben – wenngleich das bedeutet, mehrere Dutzend von Zugangsdaten zu verwalten. Wer da den Überblick verliert, für den kann ein Passwort-Manager Abhilfe schaffen.

Checkliste:

- Von E-Mail bis Social Media: Für welche Konten brauchen Sie einen Passwort-Manager?
- Browser-basiert oder eigenständig: Welches Programm passt am besten zu Ihren Online-Gewohnheiten?
- Cloud oder Festplatte: Wo werden Ihre Daten gesichert?
- Sensible Daten: Benötigen Sie einen zweiten Faktor zur Authentisierung?
- Komplexe Kombinationen: Haben Sie ein sicheres Masterpasswort?

Passwort-Manager sind Programme, die Benutzernamen und Passwörter verwalten. Mittels Verschlüsselung und eines komplexen Masterpassworts verwahren Passwort-Manager die Passwörter sicher. Sie funktionieren ähnlich wie ein Notizbuch, das in einer Schublade eingeschlossen ist und dessen Inhalte somit nur für den Besitzer oder die Besitzerin einsehbar sind. Der Vorteil liegt auf der Hand: Anstelle von vielen verschiedenen Passwörtern muss sich nur noch eins gemerkt werden.

Vorteile des Passwort-Managers

- **Verwahren von Passwörtern** und Benutzernamen mittels Verschlüsselung
- **Unterstützung bei der Passwortvergabe**: z. B. durch die Generierung starker Kombinationen und Kennzeichnung schon verwendeter oder schwacher Begriffe.
- **Warnung vor gefährdeten Websites und möglichen Phishing-Attacken**, z. B. wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.
- **Synchronisieren möglich:** Wer Online-Dienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen nutzen möchte, kann ein Programm verwenden, das diese synchronisiert.

Passwörter mit dem Passwort-Manager speichern

Je nach Wahl des Programms werden die Passwörter entweder lokal auf dem Gerät oder zwecks Synchronisierung auf verschiedene Systeme auch in der Infrastruktur des Anbieters – oftmals cloudbasiert – gespeichert.

Eigenständiges Passwort-Manager-Programm
Sind eigenständige Programme einmal aktiviert und eingerichtet, erscheint ein Pop-up-Fenster, wenn zur Nutzung eines Online-Dienstes die Eingabe von Nutzernamen und Passwort erforderlich sind. Dann muss ein zentral hinterlegtes Masterpasswort eingegeben werden, das alle Zugangsdaten schützt.

Im Browser integrierte Passwort-Manager
Viele Webbrowser bieten bereits einen integrierten Passwort-Manager an, der ohne großen Aufwand genutzt werden kann. Einmal eingerichtet, agiert er eigenständig und das Programm wird beim Aufrufen einer Website aktiv, sofern dort Zugangsdaten benötigt werden. Da Browser aber komplexe Programme sind, die dieses Thema nicht mit oberster Priorität behandeln, können die Zugangsdaten relativ einfach von Schadsoftware extrahiert und somit von einem Angreifer missbraucht werden.

Die Verwendung eines Masterpassworts bietet zwar ein Mindestmaß an Schutz, doch Anwender und Anwenderinnen sollten immer die neuesten Updates durchführen. Außerdem sollte der Zugang zum Computer, Tablet oder Smartphone gesichert werden, z. B. durch eine PIN- oder Passwort-Abfrage.

Nachteile des Passwort-Managers

- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
- Alle Passwörter können auf einmal gestohlen werden, sollte ein Cyber-Angriff auf einen Passwort-Manager erfolgreich sein.
- Bei cloudbasierten Diensten vertrauen Sie den Zugang zu all Ihren sensiblen Daten in der Regel einem Unternehmen an. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Herstellers. Die Informationen über den Standort des Cloud-Dienste-Anbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterworfen sind.

Passwörter speichern - Multifaktorauthentifizierung

Für Ihre hochsensiblen Inhalte sollten Sie im Passwort-Manager am besten einen erweiterten Schutz einrichten. Dieser lässt sich durch die Einrichtung eines zweiten Faktors bei wichtigen Accounts realisieren. Dann könnte zum Beispiel ein Bestätigungscode an ein weiteres Gerät wie Ihr Smartphone gesendet werden, um den Vorgang eindeutig zu authentisieren. Zu den wichtigen

Accounts gehören beispielsweise Ihre E-Mail-Konten. Denn wenn Dritte Zugang dazu erhalten, können diese deutlich größeren Schaden anrichten. Einerseits könnten sie auf Ihre E-Mail-Daten zugreifen, darüber hinaus auch in Ihrem Namen Nachrichten versenden. Zudem können Cyber-Kriminelle mit Zugriff auf Ihr E-Mail-Konto weitere Online-Dienste übernehmen, indem sie Passwörter darüber zurücksetzen.

Aufgeräumt ins neue Jahr: Systeme fit für 2023

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2023-01-09

Vorwort

Viele Ihrer Kunden sind zwischen den Jahren im Urlaub oder haben Betriebsferien. Der ideale Zeitpunkt also, um die Systeme einmal gründlich unter die Lupe zu nehmen und auszumisten! Wir haben 6 Tipps, wie Sie Ihre Kunden-IT wieder auf Vordermann bringen.

Tipp 1: Verschaffen Sie sich einen Überblick über das Netzwerk

Mehr Geräte, neu installierte Software, zusätzliche Daten – fast jede IT-Infrastruktur wird mit der Zeit größer. Um den Überblick zu behalten und mögliche Sicherheitslücken zu erkennen, sollten Sie regelmäßig eine Netzwerk-Inventarisierung durchführen. Sobald Sie sich ein klares Bild von der Netzwerkstruktur verschafft haben, können Sie dieses viel gezielter aufräumen.

Tipp 2: Bringen Sie die Software auf den neuesten Stand

Wird ein Programm über längere Zeit nicht aktualisiert, schränkt dies nicht nur den Funktionsumfang ein, es entstehen auch unnötige Sicherheitslücken. Prüfen Sie daher genauestens, welche Software ein Update vertragen könnte oder ganz ersetzt werden sollte.

Tipp 3: Löschen Sie inaktive Benutzer

Verlässt ein Mitarbeiter das Unternehmen, sollten auch seine Benutzerprofile entfernt werden. Eigentlich. Denn gerade in größeren Betrieben kann dieser Schritt im stressigen Tagesgeschäft schnell untergehen. Die Folge: ein unkalkulierbares Sicherheitsrisiko für das Unternehmen. Warum nicht die Zeit zwischen den Jahren dazu nutzen, diese Schwachstellen zu eliminieren?

Tipp 4: Schalten Sie stillgelegte Testumgebungen ab

Jeder kennt es: Ein Testsystem wird aufgesetzt und nach Verwendung vergessen. Vielleicht entschließt sich Ihr Kunde auch bewusst dazu, es weiterlaufen zu lassen – man könnte es ja nochmal gebrauchen. Doch mit der Zeit kann so eine größere Ansammlung entstehen, die unnötig Speicherplatz frisst und zu einer potenziellen Sicherheitslücke wird. Prüfen Sie daher genau, welches Testsystem wirklich noch gebraucht wird und welches abgeschaltet werden sollte.

Tipp 5: Misten Sie Ihre E-Mail-Postfächer aus

Durch überfüllte Postfächer werden nicht nur die Systeme überlastet, Ihre Kunden verlieren auch zusehendes den Überblick über ihre Nachrichten. Jedes Postfach von Hand aufzuräumen, kostet jedoch viel Zeit. Hier kann eine E-Mail-Archivierungslösung wie MailStore helfen: Über Löschregeln lassen sich E-Mails automatisiert aus dem Postfach entfernen, sobald sie archiviert wurden.

Tipp 6: Verschieben Sie ungenutzte Daten an andere Speicherorte

Neben den E-Mail-Postfächern sollten Sie auch die Festplatten Ihrer Kunden von Zeit zu Zeit aufräumen. Denn nur ein Bruchteil der angesammelten Daten wird im Produktivbetrieb tatsächlich benötigt. Wenn Sie ungenutzte Dateien und Ordner auf einen anderen Datenträger oder in die Cloud verschieben, setzen Sie wertvollen Speicherplatz frei.