SMART DATA CENTER

Ihre Daten in sicheren Händen – unter Kontrolle und geschützt

Foto: Gorodenkoff / shutterstock.com

Cyberattacken wirkungsvoll begegnen

Smart DataCenter

Inhaltsverzeichnis

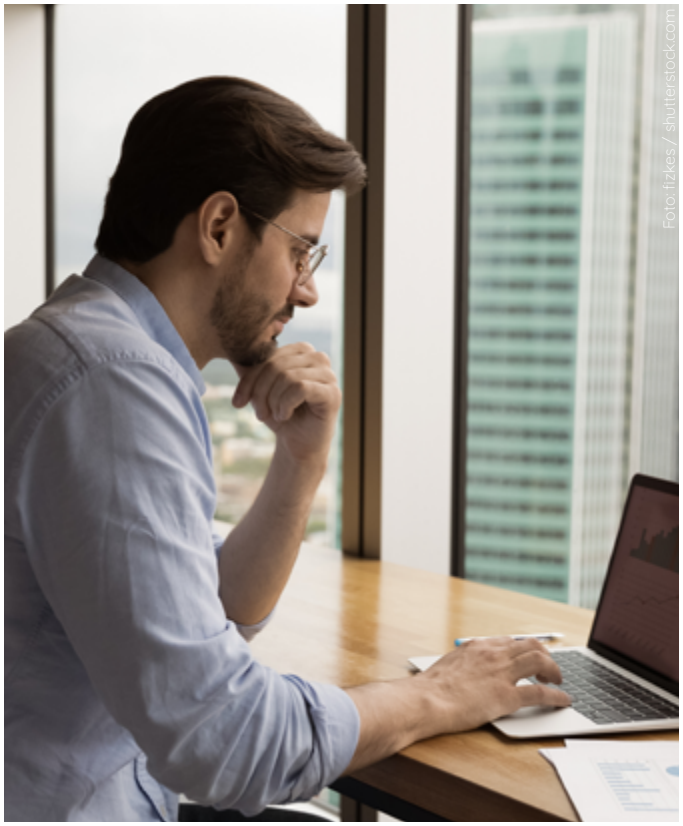

Foto: fizkes / shutterstock.com

Akute Bedrohungen durch Cyberkriminalität

Unsere Arbeitswelt entwickelt sich rasant. Neue Technologien und Innovationen verändern das Arbeiten von heute und morgen. Wer hätte vor zwei Jahren noch gedacht, dass Homeoffice und mobiles Arbeiten so schnell ein Teil unserer Arbeitskultur würden?

Heute arbeiten wir beispielsweise von unserem Zuhause auf dem Land aus, obwohl unser Büro in der Stadt liegt. E-Mails beantworten wir per Smartphone in der Bahn und an Meetings nehmen wir online teil. Es ist also egal, ob wir gerade in Singapur, New York oder Berlin sind. So weit, so gut.

Mit der Digitalisierung kommen aber auch neue Gefahren auf uns zu. Die Zahlen der Cyberangriffe von 2021 und 2022 sind erschreckend. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Bedrohung im Cyberraum so hoch wie nie. Dabei stellt die Verschlüsselung der eigenen Firmendaten durch Cyberkriminelle und eine daran anschließende Forderung nach Lösegeld eine der verbreitetsten Aktivitäten dar. Die sogenannte Ransomware entwickelt und verbreitet sich zunehmend. Im Jahr 2021 waren 47 % der angegriffenen Daten verschlüsselt.

Von diesen Daten waren nur 64 % wiederherstellbar. Das Eindringen in ein Netzwerk und die Verschlüsselung von Daten durch Ransomware wird für Cyberkriminelle immer mehr zu einer effektiven Strategie. Denn mittlerweile haben Kriminelle die Möglichkeit, im Darknet günstig Software wie z. B. Ransomware zu kaufen, mit der sie einen Angriff auf Unternehmen vornehmen können.

Dadurch ist heutzutage nicht mal mehr hoch entwickeltes Expertenwissen vonnöten, um Betriebe, Institutionen und Verbraucher*innen infiltrieren zu können. Unternehmen aller Größenordnungen versäumen es, Sicherheitslücken zu schließen oder schwache Glieder in der Sicherheitskette zu stärken. Die Fähigkeit, Daten zu schützen, um Geschäftsausfälle zu vermeiden, stellt daher eine der größten Herausforderungen für die deutsche Wirtschaft dar.

76 %

der Unternehmen waren 2021 Opfer einer Art von Ransomware-Attacke

47 %

der angegriffenen Daten waren zuvor verschlüsselt

64 %

der Daten waren nach dem Angriff nur noch wiederherstellbar

„Im Risikomanagement der IT-Sicherheit muss ein Back-up-Konzept, das nicht erfolgreich erprobt wurde, so gewertet werden, als wenn kein Back-up-Konzept existiert. Um dieses Risiko zu beherrschen, muss die vollständige Wiederherstellung aller Systeme und Daten im Rahmen einer Notfallwiederherstellung erfolgreich getestet werden. Das betrifft sowohl die technischen als auch die organisatorischen Abläufe.“

– Peer Casper, Geschäftsführer Smart Data Center GmbH

Ransomware bekämpfen

Jedes Unternehmen muss seine Daten im digitalen Zeitalter schützen – doch auch die beste Firewall und der beste Virenscanner können durchbrochen werden. Leider wird das Ergreifen von Maßnahmen zur Reduzierung der Schadenshöhe, die durch einen Ausfall der IT-Infrastruktur entsteht, noch immer unterschätzt. Die komplementären Lösungen von Smart Data Center bewahren Sie vor Geschäftsunterbrechungen und arbeiten am besten zusammen, wenn etwas Unerwartetes passiert – Cyberangriffe, Insider-Bedrohungen, Hardware-Ausfälle oder Naturkatastrophen.

Foto: Gorodenkoff / shutterstock.com

Back-up as a Service (BaaS)

Viele Unternehmer*innen unterschätzen die Wichtigkeit funktionierender Back-up-Strategien. Es muss jederzeit gewährleistet sein, dass alle Daten, inklusive der Betriebssysteme, reibungslos wiederhergestellt werden können. In der Praxis bedeutet dies, dass Sie mindestens eine Sicherungskopie an einem externen Standort haben sollten – Ihr Back-up. Durch diese Kopie können Sie Ihre Unternehmensdaten zurückholen, sollten diese durch einen Virus oder eine Cyberattacke beschädigt oder vernichtet worden sein.

Unser Back-up as a Service (BaaS) ist eine kostengünstige und einfache Möglichkeit, die Daten Ihres Unternehmens bei Smart Data Center zu sichern. Während herkömmliche Back-ups nur die Daten schützen, sichern wir Ihre gesamte IT-Infrastruktur in der Cloud. Dazu gehören etwa die Betriebssysteme und das Netzwerk für den Zugriff und die Wiederherstellung. Zudem kümmern sich unsere Expert*innen um die Administration und stellen mit regelmäßigen Restore-Tests sicher, dass sämtliche Bereiche Ihres Unternehmens jederzeit über ein System-Back-up fehlerfrei wiederhergestellt werden können.

- *Automatische Sicherung Ihrer kompletten IT-Infrastruktur inkl. Daten und Betriebssystemen*
- *Rechenzentren made in Germany sowie DSGVO-konform*
- *Überwachung und Berichterstattung über den Status der Sicherung*
- *Umfassende Datenverschlüsselung*
- *Redundanz und Ausfallsicherung für schnelle Wiederherstellung*
- *Einfache Bereitstellung und Verwaltung*
- *Umwandlung von Investitionskosten in Betriebskosten*

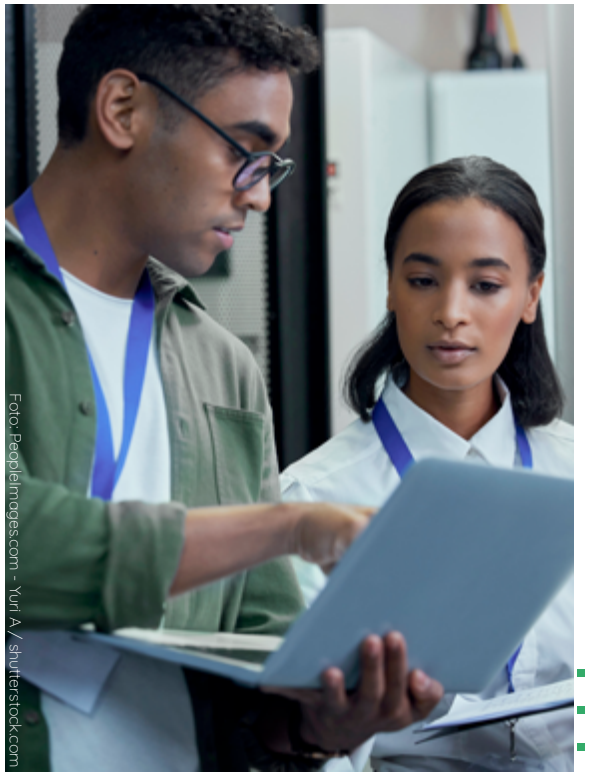

Foto: PeopleImages.com - Yuri A / shutterstock.com

Disaster Recovery as a Service (DRaaS)

Dank DRaaS ist Ihr Unternehmen auch im Katastrophenfall abgesichert. Das bedeutet: Sollte Ihre IT durch Ransomware-Attacken oder Umwelteinflüsse lahmgelegt werden, greift die Wiederherstellungssoftware von Smart Data Center ein und stellt sämtliche Back-ups in einer sicheren Umgebung wieder her. Nur so kann gewährleistet werden, dass Ihr Unternehmensalltag ohne große Ausfälle und Probleme weitergeführt werden kann.

DRaaS nutzt virtuelle Server, um Ihre komplette IT-Infrastruktur (Rechen-, Speicher- und Netzwerkfunktionen) im ausfallsicheren Modus zu spiegeln. So können Sie als Unternehmen Ihre Geschäftsanwendungen weiterhin in einer geschützten Cloud-Umgebung von Smart Data Center ausführen, ohne gefährdete Server vor Ort nutzen zu müssen. Das Ergebnis ist eine schnelle, nahezu sofortige Wiederherstellung nach einer Katastrophe.

- *Kostengünstige Disaster-Recovery-Lösung*
- *Nahezu sofortige Wiederherstellung der kompletten IT-Umgebung*
- *Keine zusätzliche Infrastruktur nötig*
- *Automatisiertes und erprobtes Back-up-Konzept*
- *Überprüfung, ob die Sicherungen virenfrei sind, bevor sie wiederhergestellt werden.*
- *Vereinfachte, vollständig orchestrierte DR*

Foto: Gorodenkoff / shutterstock.com

Desktop as a Service (DaaS)

Mithilfe eines Desktop as a Service, also einem virtuellen Desktop, lassen sich viele Herausforderungen des digitalen Zeitalters an Ihre IT-Abteilung meistern. Mit unseren virtuellen Desktops wird das Betriebssystem hardware- und ortsunabhängig in der Cloud von Smart Data Center ausgeführt – lediglich die grafische Oberfläche wird auf Ihrem Endgerät angezeigt.

Foto: tsingho25 / shutterstock.com

Da Ihre Daten nicht mehr auf lokalen Geräten gespeichert werden, sind diese orts- und zeitunabhängig abrufbar. Das bedeutet: Auch bei einem Unglück – einem Unfall oder Angriff auf die lokalen Systeme – bleiben die Daten sicher und sind vor Cyberangriffen zusätzlich geschützt.

Weiterhin werden alle virtuellen Desktops durch Smart Data Center automatisch aktualisiert und gewartet. Ebenso können Administrator*innen auf alle virtuellen Desktops innerhalb des Unternehmensnetzwerkes zugreifen, um neue Software zu installieren und einzurichten. Der On- und Offboarding-Prozess von Mitarbeitenden kann so einfacher organisiert werden. Dynamisch wachsende Unternehmen haben die Möglichkeit einer einfachen Skalierbarkeit – per Mausklick können beispielsweise 20 neue Arbeitsplätze gleichzeitig erstellt werden. Ohne großen Aufwand und hohe Kosten. Investitionen in teure Hardware, die alle paar Jahre erneuert werden muss, gehören damit der Vergangenheit an.

- *Schneller, kostengünstiger Einsatz*
- *Gute Skalierbarkeit und Flexibilität*
- *Office- und Groupware-Lizenzierung*
- *Benutzer*innen benötigen keine rechenstarken Endgeräte, da diese nur noch die Darstellung ausführen, also anzeigen und nicht berechnen müssen.*
- *Sie und Ihre Mitarbeitenden können sich von jedem Gerät und an jedem Ort mit einer Internetverbindung einloggen.*
- *Alle Anwendungen und Daten Ihres Unternehmens sind mit den integrierten intelligenten Sicherheitsfunktionen bestmöglich gegen Cyberkriminalität geschützt.*
- *Automatische Back-ups schützen Ihre Daten vor Verlust.*
- *Auch wenn das Gerät, auf dem Sie arbeiten, mit einem Virus befallen ist, kann dieser nicht den virtuellen Desktop angreifen.*

Cyberangriffe und wie Sie sich wirklich schützen können

Interview mit Peer Casper, Geschäftsführer Smart Data Center GmbH

Wie funktioniert der professionelle und sichere Schutz vor Hacker*innen?

Um ruhig schlafen zu können, obwohl die Cyberkriminalität ständig wächst, wenden Profis Methoden aus dem Risikomanagement an. Dabei kommen zwei Techniken gleichzeitig zum Einsatz. Einerseits beschäftigt man sich ausschließlich mit der Reduzierung des Risikos, überhaupt gehackt zu werden.

Welche Maßnahmen können einen Cyberangriff verhindern?

Maßnahmen, um Cyberangriffe zu verhindern, wären zum Beispiel der Einsatz von modernsten und stets aktuellen Virenscannern sowie Firewalls. Auch Mitarbeiterschulungen zum Schutz vor Phishing-Mails sind äußerst wichtig. Weitere Maßnahmen beinhalten die Nutzung von aktuell gepflegter Software, automatische Updates, einen sorgsamen Umgang mit den Superuser-Rechten (Admin), präzise Mindestanforderungen sowie Tests für sämtliche eingesetzte Software und vieles mehr.

Welches ist die zweite Technik, die Unternehmen einsetzen können?

Dies sind alles wichtige und bekannte Dinge. Jedoch werden diese selten perfekt durchgeführt. Deshalb beschäftigt man sich im zweiten Teil dann mit dem sehr unangenehmen Fall, dass Sie trotz aller getroffenen Maßnahmen dennoch gehackt wurden und von einem Totalverlust aller Daten in Ihrem Unternehmen konkret bedroht sind. Dabei kommt der Sicherung aller Daten und Systeme eine entscheidende Rolle zu.

Viel wichtiger ist es jedoch, überhaupt erst einmal zu testen, ob die getätigten Datensicherungen zu einer vollständigen Wiederherstellung aller Daten und Systeme führen. Rund 99 % aller mittelständischen Unternehmen haben bisher auf diesen Schutz meist aufgrund von Unkenntnis, Kostengründen oder mangelnden technischen Möglichkeiten verzichtet.

Wieso ist dieser Test so wichtig? Haben Sie ein vergleichbares Beispiel?

Würden Sie in einem Flugzeug einen Transatlantikflug beginnen, wenn Ihnen beim Einsteigen gesagt wird, dass definitiv weder die Pilot*innen noch Sie selbst geprüft haben, ob für den weiten Flug genug Benzin im Tank sei? Sicher nein, aber genau dies ist der reale Fall in Millionen mittelständischen Betrieben. Denn von rund 3,3 Millionen Unternehmen in Deutschland führen die wenigsten regelmäßig eine vollständig funktionierende Datensicherung durch. Dabei ist dies eine extrem wichtige Maßnahme, sollten Daten verschlüsselt worden sein. Wenn ein*e Hacker*in Sie erpresst und selbst bei Lösegeldzahlung nicht klar ist, ob Sie Ihre Daten zurückerhalten, dann hilft nur eines: ein vollständiges, vor allem funktionierendes Back-up. Ein paar Fakten zum Wachrütteln wären zum Beispiel, dass über 99 % aller Firmen Datensicherungen betreiben, jedoch über 99 % aller Firmen noch nie selbst getestet haben, ob diese eigene Datensicherung überhaupt funktioniert. Das bedeutet, jede*r macht Datensicherungen, aber keine*r testet, ob diese am Ende funktionieren und der Betrieb reibungslos weiterlaufen kann. Wer in der Cybersicherheit etwas nicht ausprobiert hat, darf nur davon ausgehen, dass er keine Cybersicherheit hat.

Was müssen Unternehmer*innen also durchführen, um auf der sicheren Seite zu sein?

Alle Unternehmer*innen (und ab jetzt bitte unbedingt auch Sie!) sollten so schnell wie möglich testen, ob die eigene Datensicherung wie vorgesehen eine funktionierende Wiederherstellung Ihrer Systeme ermöglicht. Schätzungsweise ist dies bei zwei Drittel aller in Deutschland vorhandenen Datensicherungen leider nicht der Fall. Diese sind im Grunde völlig wertlos und niemand ist sich dessen bewusst.

Warum machen so viele Unternehmen diesen Test nicht einfach?

Die meisten Menschen und ebenfalls die meisten IT-Spezialist*innen sind keine Datensicherheitsexpert*innen. Viele Unternehmen sind schlicht und einfach oft noch nicht auf die Idee gekommen, diesen Test zu machen. Wir kennen auch niemanden,

der uns darauf hinweist und uns warnt, keinesfalls ohne einen erfolgreichen Wiederherstellungstest in die Zukunft zu gehen. Zusätzlich ist der Test eines Back-ups viel schwieriger und aufwändiger, als es den Anschein macht. Back-ups auf Funktionsfähigkeit zu testen, ist aktuell noch wenigen großen Konzernen vorbehalten, die für diese Sicherheit sieben- bis achtstellige Beträge pro Jahr investieren (müssen).

Was wird bei einem Test der Datensicherung benötigt?

Der Test der eigenen Datensicherung ist nur möglich, wenn Sie jedes Hardware-Gerät, jeden Rechner, jeden Server, jedes Telefon, jedes Tablet und jedes Notebook doppelt besitzen, laufend professionell updaten und administrieren.

Das bedeutet: Sie benötigen für absolut jedes Gerät Zwillinge, Ihre Hardwarekosten verdoppeln sich dadurch. Die meisten Firmen wissen also nicht, wie das geht, und wenn man den Geschäftsführer*innen mitteilt, dass eine ewige Verdopplung der Hardwarekosten ansteht, wird man dort auch nicht auf Begeisterung stoßen. Tatsächlich unterhalten wenige große Konzerne ganze Turnhallen voller „Zwillingshardware“, in denen jeden Tag Profis auf jedem Zwillingsgerät dieselben Updates erledigen, welche im Hauptgerät Tag für Tag installiert werden. Nur wer identische Technik mit dem identischen Stand der Software hat, wird überhaupt eine gute Chance haben, dass sein Back-up von Erfolg gekrönt sein wird.

Was bietet Smart Data Center seinen Kund*innen?

Wir, die Smart Data Center GmbH, haben erstmals eine Lösung ohne teure Zwillingsgeräte entwickelt. Jede*r unserer Kund*innen darf einmal im Jahr im Rahmen der normalen monatlichen Miete sein eigenes Back-up selbst und vollständig testen. Nur so erhalten Sie die Sicherheit, dass das, was für Ihren Betrieb im schlimmsten Fall überlebenswichtig sein wird, auch wirklich funktioniert. Dieser von den Expert*innen für Rechenzentren auch „Disaster Recovery Test“ genannte Vorgang ist von allen Schutzmaßnahmen gegen Cyberkriminalität der mit weitem Abstand allerwichtigste! Selbst wenn Sie keine gute Vorsorge gegen Kriminelle getroffen haben (was wirklich nicht empfehlenswert ist), so hilft Ihnen die Gewissheit, immer wieder den gesamten System- und Datenbestand Ihres Unternehmens

Foto: Peoplelmages.com - Yuri A / shutterstock.com


Foto: everything possible / shutterstock.com

sicher und schnell wiederherstellen zu können. Ihr Unternehmen ist dann zwar immer noch erpressbar – aber Sie werden nie mehr zahlen müssen! Egal, was Sie sonst machen – auf den regelmäßigen Test Ihrer eigenen Datensicherung sollten Sie ab sofort niemals mehr verzichten.

Warum weiß davon niemand / warum hat mir das mein*e IT-Chef*in nicht gesagt?

Nun, vermutlich gehört auch Ihr*e IT-Chef*in nicht zu den nur sehr, sehr wenigen Expert*innen für Rechenzentren in Europa. Seit 40 Jahren sichern sich wenige Vollprofis sehr teuer und aufwändig über die oben beschriebene Zwillingslösung ab. Der gesamte Mittelstand hingegen macht Datensicherungen, ohne dieselben jemals ausprobiert zu haben. Da es bis vor 18 Monaten kaum kriminelle Hacker*innen gab, hat das niemanden gestört.

Wenn man bei dem vorherigen Beispiel mit dem Transatlantikflug bleibt, bedeutet dies, wir starten, ohne vor Abflug den Kerosinstand in unserem Flugzeug überprüft zu haben. Einfach nur, weil das seit 40 Jahren überall gut gegangen ist, empfinden weder Sie noch die meisten Anderen dieses Vorgehen für ungewöhnlich oder halten es sogar für falsch. Ähnlich ist es beim Thema Cybersicherheit. Erst seit rund 1,5 Jahren kann jede*r Kriminelle im Darknet innerhalb von wenigen Stunden und ohne Vorkenntnisse Viren, E-Mail-Adressen von Mitarbeitenden, Erpressungssoftware und Bitcoin-Konten für wenig Geld erwerben.

Aus diesem Grund haben wir es mit einer neuen Bedrohung zu tun. Erst wenn 10.000 Firmen in Deutschland aufgrund einer Erpressung Insolvenz anmelden mussten, rechnen wir mit einem flächendeckenden Umdenken in den Führungsetagen deutscher Betriebe bundesweit.

Was raten Sie allen Unternehmen?

Unternehmen sollten sich drei Dinge bewusst machen: Sie sollten nicht länger Aussagen vertrauen – von wem auch immer diese erfolgen mögen –, dass Ihre Firma gut geschützt sei. Außerdem sollten Sie den Schutz Ihrer Daten und zusätzlich Ihr eigenes Back-up testen. Nur dann können Sie ruhig schlafen und erfüllen Ihre Verantwortung gegenüber allen Eigentümer*innen, aber auch gegenüber Ihren Mitarbeiter*innen und Kund*innen.

Dank unserer innovativen High-Tech-Lösung testet jede*r unserer Kund*innen vollständig automatisiert seine/ihre eigene Datensicherung einmal pro Jahr ohne Mehrkosten (monatlicher Test optional möglich). Mit wenig Aufwand werden Sie sich als Unternehmer*in wieder sicher fühlen können!

Treffen Sie noch heute die wichtigste Entscheidung für die Sicherheit Ihres Unternehmens: Werden Sie Kund*in von Smart Data Center und testen Sie ab sofort regelmäßig Ihre Datensicherungen auf Funktion.

Foto: fizkes / shutterstock.com

Ihre Adresse für Cybersicherheit

Smart Data Center GmbH
Südportal 3
22848 Norderstedt

E-Mail
kontakt@smart-datacenter.de

Telefon
+49 40 741 24 16 0