IT-Sicherheit

Risiken minimieren,
Verfügbarkeit maximieren.

business.ewe.de/it-security

EWE

Inhalt

1. Die Bedeutung von IT-Sicherheit für Unternehmen

Gefahren und Folgen werden unterschätzt
Die Ausfallsicherheit der Informationstechnologie (IT) ist für jeden Betrieb von Bedeutung. In manchen Unternehmen werden die Risiken unterschätzt, weil alles reibungslos läuft. Dies gilt insbesondere für kleine und mittlere Unternehmen. Spätestens nach dem ersten Cyberangriff oder einem IT-Ausfall, der sich nicht auf die Schnelle wieder beheben lässt, ändert sich das schlagartig.

1.1 Warum Ausfallsicherheit und Informationssicherheit so wichtig sind

Wichtige Prozesse laufen über die IT
Die IT muss funktionieren, und das im gesamten Unternehmen. Fällt sie zum Beispiel in der Produktion, bei Kassensystemen oder im Onlinehandel aus, kann das zu empfindlichen Umsatzeinbrüchen führen, die vor allem bei kleineren Unternehmen und im Mittelstand existenzgefährdend werden können. Cyberangriffe bedeuten Betriebsstörungen, Datenverluste und oft auch hohe Lösegeldforderungen. Deshalb sollten Unternehmen sich adäquat davor schützen.

„IT" findet sich in vielen Unternehmensbereichen
Heute stützen sich bei fast allen Unternehmen wichtige Geschäftsprozesse auf IT. Das beginnt bei der Automatisierung in der Produktion, geht über die Kommunikation mit der Kundschaft sowie mit Zuliefer- und Diens tleistungsbetrieben bis hin zu Logistik und Handel. Außerdem werden sensible Daten zunehmend in der Cloud abgespeichert, auf die viele Mitarbeitende per Laptop, Tablet oder Smartphone von zu Hause oder vor Ort beim Kunden zugreifen. Damit erhält die Internetanbindung einen deutlich höheren Stellenwert als bisher.

1.2 Vielfältige IT-Gefahren und ihre Auswirkungen auf diverse Branchen

Mehr Digitalisierung, mehr Risiken
Im Zuge der zunehmenden Digitalisierung tragen auch Arztpraxen, Therapieeinrichtungen, Notariate, Steuer- und Rechtsanwaltskanzleien oder kommunale Behörden höhere IT-Risiken. Daher benötigen sie sichere Verbindungen zu speziell abgesicherten Branchen-Clouds, in denen sie sensible Personendaten abspeichern. Bei Bedarf müssen sie jederzeit auf diese Daten zugreifen können. Funktioniert die Internetverbindung nicht oder sind Server, PCs und Router wegen eines Stromausfalls nicht nutzbar, hat beispielsweise das Praxispersonal bei einer Behandlung keine Möglichkeit, auf die Patientenakte zuzugreifen. Notariate, Steuer- und Rechtsanwaltskanzleien oder Behörden wiederum haben keinen Zugang zu Urkunden, Elster-Daten oder Akten in der Cloud, was die Arbeitsabläufe behindert.

Personen- und Kundendaten besonders sensibel
Folgenreich wird es auch, wenn bei einer Cyberattacke sensible Personendaten abhandenkommen. Das kann zum Beispiel über nicht ausreichend abgesicherte Internetverbindungen geschehen oder wenn eine Sicherheitslücke bei einer genutzten Software nicht geschlossen wurde, obwohl entsprechende Sicherheitsupdates längst verfügbar sind. Solche Vorfälle beschädigen den Ruf von Arztpraxen, Kanzleien oder Behörden erheblich und können hohe Bußgelder mit sich bringen. Aus diesem Grund legen auch Finanzdienstleister großen Wert auf die sichere Übertragung und Speicherung von sensiblen Kundendaten.

Im Handel beeinflusst ein Ausfall alle Prozesse
Im Handel sind die verteilten Kassensysteme in den Filialen in der Regel an die zentrale Unternehmens-IT angeschlossen – zum einen, um die Umsätze korrekt zu erfassen, zum anderen, weil zum Beispiel das Warenwirtschaftssystem über die Informationen aus den Verkäufen eine Meldung ausgeben kann, wann welche Waren nachgeordert werden müssen. Fällt hier eine Komponente aus, kann nicht abkassiert werden, und das IT-System erfasst die Umsätze nicht mehr. Das wirkt sich nicht nur auf den konkreten Umsatz vor Ort aus, sondern auch auf Prozesse in der Lieferkette.

» Netzausfälle und Datenmanipulationen können zu massiven Störungen von Liefer- oder Steuerabläufen bis hin zum Maschinenstillstand führen. «

Produktion und Fertigung ohne IT nicht mehr denkbar
Insbesondere bei produzierenden Betrieben sind Materiallieferungen und Herstellungs- oder Weiterverarbeitungsprozesse eng aufeinander abgestimmt. Deshalb sind Standortinformationen zu Lieferungen oft entscheidend für die Planung von Prozessen. Ähnliches gilt für die automatisierte Fertigung, bei der die Positionierung von Bauteilen auf IoT-Sensoren basiert und die zugehörige Steuerung für Machine Learning oft mit einer Cloudplattform verbunden ist. Kommt es zu Netzausfällen oder zur Datenmanipulation durch Hacker, kann das zu massiven Störungen von Liefer- oder Steuerabläufen bis hin zum Maschinenstillstand führen.

2. IT-Ausfälle: Unterschiedlichste Ursachen mit großer Wirkung

Risiken und Gefahren oft aus unvermuteten Richtungen
Es gibt zahlreiche neuralgische Punkte, die die IT lahmlegen können. Nicht selten sind es technische Fehler, mit denen niemand rechnet – und die man auch schlecht vorhersehen kann. Ebenso wie die Cyberkriminalität, die immer wieder neue Angriffspunkte und Einfallstore findet.

Wichtig ist es, vorbereitet zu sein. Denn aus welcher Richtung die Gefahr auch kommt, ein Plan B oder ein geeigneter Schutz bewahren das Unternehmen vor gravierenden Folgen.

2.1 Ausfallfolgen: Auswirkungen können Existenz bedrohen

Verantwortliche machen sich über Ursachen und Folgen kaum Gedanken
Auslöser für IT-Ausfälle sind oft schadhafte Verbindungen etwa durch Baggerarbeiten, bei denen eine Leitung durchtrennt wird, oder durch Gerätedefekte, die sich mehr oder weniger schnell beheben lassen.

Ursachen können aber auch längere Stromausfälle, Vandalismus bei einem Einbruch, ein Brand oder Naturkatastrophen wie Überschwemmungen sein. Diese haben weitreichendere Folgen, da die davon betroffenen Geräte und Infrastrukturen danach unter Umständen nicht mehr einsetzbar sind.


Bauarbeiten sind häufig Ursache für IT-Ausfälle

Zwei Beispiele:

1. Ein **Stromausfall** hat die Server eines Küchenherstellers mit irreparablen Schäden lahmgelegt und zu einem **totalen Datenverlust** geführt. Das mittelständische Unternehmen konnte daraufhin für Wochen keine Aufträge mehr bearbeiten und an die Produktion weiterleiten. Es musste Insolvenz beantragen.

2. Ähnlich katastrophal können sich **Cyberangriffe** auswirken. Anfang 2023 legte eine Attacke das IT-System eines Fahrradherstellers wochenlang lahm. Auch für dieses Unternehmen bedeutete dies **fast die Insolvenz,** die dank eines Investors abgewendet werden konnte.

2.2 Cybervorfälle: Bedrohung durch vielfältige Angriffsszenarien

Immer neue Sicherheitslücken und Cybertricks
Als Hauptbedrohung gelten derzeit Ransomware-Angriffe, bei denen Cyberkriminelle Firmendaten verschlüsseln und erst wieder freigeben, wenn ein Lösegeld gezahlt wurde.

Hinzu kommen Schadsoftware, Sicherheitslücken in der Software oder auch Distributed-Denial-of-Service-(DDoS-)Attacken. Bei dieser Angriffsvariante überfluten Anfragen von verschiedenen Stellen aus dem Internet einen Server so stark, dass dieser nicht mehr ansprechbar ist. Trifft solch eine Attacke zum Beispiel die Internet-Anbindung eines Unternehmens, ist es in seiner Kommunikation weitgehend von der Außenwelt abgeschnitten: Mitarbeitende können zum Beispiel keine E-Mails mehr versenden und empfangen, und die Telefonie funktioniert nicht mehr.

Ist der Server eines Onlineshops davon betroffen, steht dieser – und damit auch der Onlineshop – aufgrund der überlasteten Verbindung erst einmal nicht zur Verfügung, was gerade an verkaufsstarken Tagen fatal ist.

Auch Phishing-Tricks weiten sich aus
Neue Technologien und Methoden wie künstliche Intelligenz, aber auch die extrem gestiegene digitale Kommunikation sorgen für noch mehr Gefahr.

Phishing-Attacken, über die Cyberkriminelle meist Zugangsdaten ausspähen, finden heute nicht mehr nur per E-Mail statt, sondern auch über Messengerdienste oder Social-Media-Plattformen.

3. Die Top-Risiken für Unternehmen in Deutschland

Die Ausführungen der vorhergehenden Seiten machen deutlich, wie wichtig Informationssicherheit für eine sichere Digitalisierung ist. Deshalb sollten Unternehmen die Ausfallsicherheit sowie die Cybersicherheit ihrer IT im Fokus haben. Einen hundertprozentigen Schutz gibt es zwar nicht, aber in der Regel lassen sich die Kernkomponenten der IT sehr gut vor Ausfällen und Angriffen schützen.

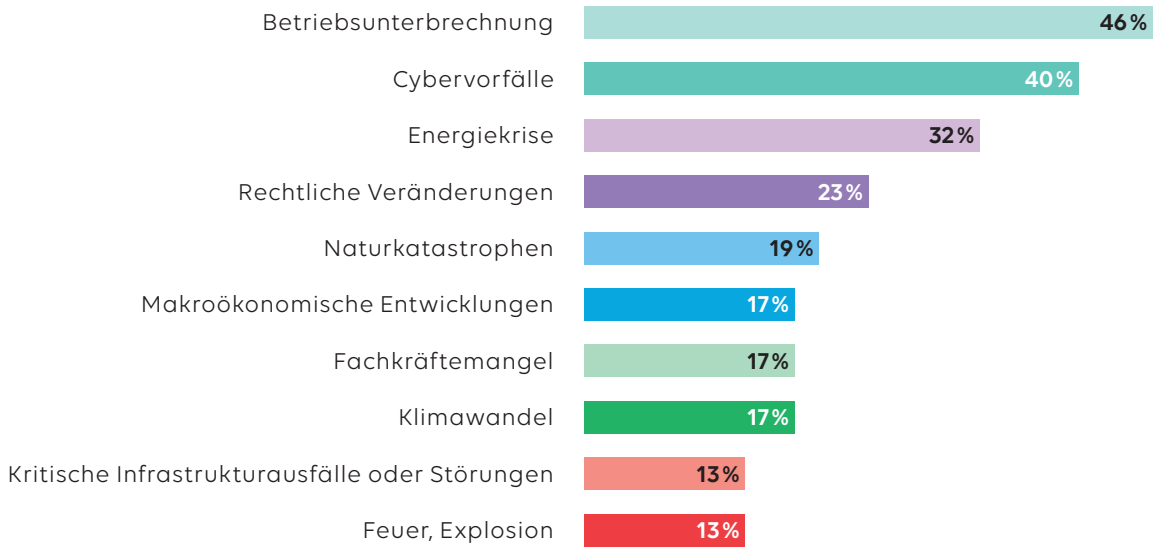
Zu diesem Ergebnis kommen auch die Risikomanagementexpertinnen und -experten, die für das „Allianz Risk Barometer 2023" Fragen zu den derzeit größten Risiken für Unternehmen beantwortet haben.

Die Ergebnisse wurden im Januar 2023 veröffentlicht: Wie bereits im Vorjahr sehen die weltweit rund 2.700 Befragten Betriebsunterbrechungen und Cybervorfälle als die Top-Risiken für Unternehmen an. Das entspricht jeweils 34 Prozent der Nennungen. Die 925 Teilnehmenden aus Deutschland schätzten diese Risiken sogar noch höher ein: Betriebsunterbrechungen erreichten hier 46 Prozent und Cybervorfälle 40 Prozent der Nennungen.

Hohe Kosten befürchten vor allem kleine und mittlere Unternehmen

Die Auswertung der Befragung ergab auch, dass vor allem kleine und mittlere Unternehmen Angst vor Cyberangriffen haben. Der Grund: die hohen Kosten durch Betriebsunterbrechungen und Lösegeldforderungen. Laut einer Umfrage vom Statista Research Department im Sommer 2022 lagen die durchschnittlichen Kosten und Verluste (Median) für eine Cyberattacke weltweit bei 15.255 Euro, in Deutschland sogar bei 18.712 Euro.

Top 10 der Geschäftsrisiken in Deutschland in 2023*



*Quelle: Allianz Risk Barometer 2023. Die Zahlen stellen den Prozentsatz der Antworten aller Teilnehmer dar, die geantwortet haben (925). Die Zahlen addieren sich nicht zu 100 %, da mehr als ein Risiko ausgewählt werden konnte.

4. Strengere Cybersicherheitsvorschriften durch NIS-2-Richtlinie für deutsche Unternehmen

Viele Unternehmen und Kommunen müssen sich besser aufstellen
Die Europäische Kommission hat im Januar 2023 mit der NIS-2-Richtlinie strengere Cybersicherheitsvorschriften verabschiedet, die das Cybersicherheitsniveau in der EU anheben sollen.

Die Vorschriften betreffen jetzt nicht mehr nur Bereiche mit kritischen Infrastrukturen, sondern auch deutlich mehr Branchen, Berufsgruppen und Unternehmen. Dazu zählen mittelständische Firmen im Lebensmittelbereich, in der Chemie- und Pharmaindustrie sowie Medizintechnik und die „öffentliche Hand".

Spätestens im Herbst 2024 müssen die Regelungen in den Mitgliedsländern in nationales Recht umgesetzt sein.

Bis dahin sollen die betroffenen Unternehmen und Kommunen technische, operative und organisatorische Maßnahmen ergriffen haben, um die Cybersicherheitsrisiken zu bewältigen und die Auswirkungen potenzieller Sicherheitsvorfälle zu verhindern beziehungsweise so gering wie möglich zu halten.

Dafür ist laut NIS-2 ein umfassendes IT-Security-Management notwendig. Doch das benötigt heute im Grunde jedes Unternehmen, dessen Geschäftserfolg weitgehend von der IT und einer funktionierenden Internetanbindung abhängt.

5. Hochverfügbarkeit: Wie Unternehmen eine ausfallsichere IT-Infrastruktur aufbauen

Durchgängige Verfügbarkeit ist das Ziel
Bei einer ausfallsicheren IT-Infrastruktur muss das Netzwerk mit den angeschlossenen Geräten und den darauf laufenden Diensten und Softwarelösungen möglichst durchgängig verfügbar sein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Verfügbarkeit im IT-Grundschutz folgendermaßen: „Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können."

Verfügbarkeitsklassen: definiert durch die jeweils tolerierte Ausfallzeit
Eine verfügbare Infrastruktur hat einen normalen bis hohen Schutzbedarf und entspricht in der Regel der Verfügbarkeitsklasse 2. Doch Verfügbarkeitsklassen können für verschiedene Dienste und Infrastrukturen je nach Branche und spezifischen Anforderungen unterschiedlich definiert werden. Das gilt auch für Internetanbindungen.

Beispiel für eine gängige Einteilung in Verfügbarkeitsklassen

Verfügbarkeitsklasse	Verfügbarkeit	maximale Ausfallzeit
2	99 %	< 3 Tage, 15 h, 40 min
3	99,9 %	< 8 h, 46 min
4	99,99 %	< 5 min

In der Regel spricht man bei dieser Einteilung ab Verfügbarkeitsklasse 3 von einem hochverfügbaren Netz oder IT-System.

Service Level Agreements regeln Verfügbarkeitsklassen
Wenn ein Unternehmen einen Service Provider beauftragt, sollte es im Dienstauftrag über Service Level Agreements (SLAs) festhalten, welche der vorab definierten Verfügbarkeitsklasse für die einzelnen IT-Systeme und Dienste erforderlich ist.

Um später in der Umsetzung die geforderte Verfügbarkeit eines IT-Systems oder Netzwerks zu erreichen, müssen diese mehr oder weniger redundant ausgelegt werden. Das heißt, dass beim Ausfall einer Komponente oder Leitung auf eine zweite umgeschaltet werden kann, sodass keine Betriebsunterbrechung auftritt.

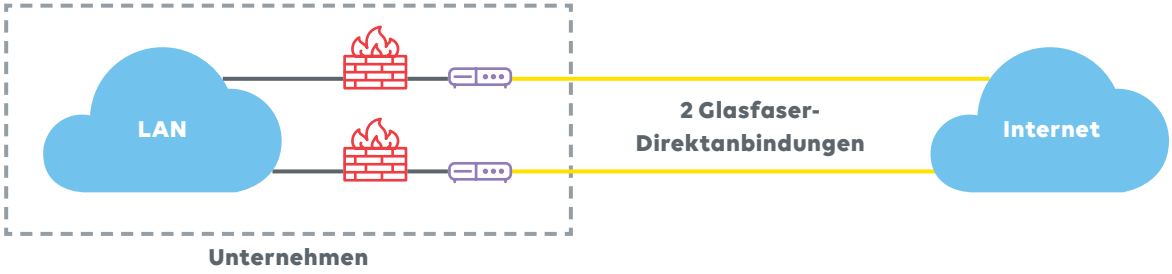
Hier hat die IT-Branche entsprechend den Verfügbarkeitsklassen mehrere Redundanzklassen festgelegt, um die geforderte Verfügbarkeit zu erreichen. Redundanzklassen beschreiben somit, welche Komponenten auf welche Weise redundant ausgelegt werden müssen, um die geforderte Verfügbarkeit zu erreichen.

5.1 Internet: Ausfallsicherheit durch Redundanz

Redundanzkonzepte für unterschiedliche Anforderungen
Eine redundante Internetanbindung ist eine wichtige Komponente für die hohe Verfügbarkeit von Online-Diensten. Um Redundanz zu erreichen, verwenden Provider zwei oder mehr separate Verbindungen. Bei Störung oder Ausfall schaltet das System automatisch auf die alternative Verbindung um. Dieser Schutzmechanismus reduziert das Risiko für Verbindungsunterbrechungen erheblich und gewährleistet eine nahtlose Vernetzung.

Je nach Anforderungen und Budget stehen verschiedene Redundanzkonzepte zur Verfügung: von der Verwendung doppelter Netzwerkkomponenten wie Switches, Router oder Firewalls beim Netzanschluss des Unternehmens und beim Provider bis hin zu Wege- und Trassenredundanz. In diesem Fall werden die Daten über verschiedene Kabel und Leitungswege transportiert, um die Wahrscheinlichkeit von Ausfällen durch Kabelbrüche, Bauarbeiten oder Naturkatastrophen zu minimieren.

Eine Kombination von mehreren Redundanzoptionen erhöht die Ausfallsicherheit noch zusätzlich. Wenn beispielsweise sowohl die Netzwerkkomponenten im Gebäude als auch die Trassen- und Wegeredundanz vorhanden sind, sinkt dadurch das Ausfallrisiko erheblich.



Zwei Glasfaser-Direktverbindungen werden über zwei separate Hausanschlüsse geleitet. Diese Verbindungen haben keine physische Überlappung und nutzen zwei verschiedene Anknüpfungspunkte zum Internet, während das gleiche IP-Netzwerk verwendet wird.

Entscheidend für Unternehmen ist die für sie passende Kombination von Redundanzlösung und Anbindungsart entsprechend den Anforderungen, Risikotoleranzen und des Budgets. Um einen effizienten und zuverlässigen Betrieb zu gewährleisten, müssen redundante Internetverbindungen sorgfältig geplant und konfiguriert werden.

Ein erfahrener Netzwerkexperte oder IT-Dienstleister kann bei der Implementierung und Konfiguration dieser Redundanzoptionen helfen, um sicherzustellen, dass das Internetverbindungsrisiko minimiert und ein hoher Grad an Hochverfügbarkeit erreicht wird.

TIPP: Mit Internet-Direktanbindung Verfügbarkeit erhöhen

Sogar die Art der Internetverbindung hat Einfluss auf deren Ausfallsicherheit. Direktanbindungen beispielsweise bieten im Vergleich zu DSL- oder FTTH-Anbindungen eine höhere garantierte Verfügbarkeit. Die direkte physische Verbindung zum Netzwerkknotenpunkt minimiert die Anfälligkeit für Ausfälle durch externe Faktoren. Die Stabilität und Zuverlässigkeit einer Direktanbindung wird durch ihre dedizierte Natur unterstützt, da sie ohne andere Benutzer oder Lastspitzen arbeitet.

5.2 Cybersicherheit: Die wichtigsten Schutzmaßnahmen

Neben der Redundanz gibt es weitere Sicherheitsmaßnahmen, die heutzutage unverzichtbar sind. Im Folgenden eine kurze Erläuterung der wichtigsten Anwendungen:

✓ **Firewall:** Diese zählt zum Basisschutz, sie überwacht den Datenverkehr zwischen Netzwerk und Internet und blockiert unautorisierten Zugriff. Sie stellt sicher, dass nur vertrauenswürdiger Datenverkehr ins Unternehmensnetzwerk gelangt. Durch die Konfiguration einer Firewall lassen sich der Datenverkehr kontrollieren sowie bekannte Bedrohungen abwehren.

✓ **Professioneller Antivirenschutz:** Unerlässlich, um die Unternehmens-IT vor schädlicher Software zu schützen. Eine zuverlässige Antivirensoftware erkennt und entfernt Viren, Trojaner, Spyware und andere schädliche Programme. Regelmäßige Aktualisierungen der Antivirensoftware stellen sicher, dass die IT stets vor den neuesten Bedrohungen geschützt sind. Darüber hinaus müssen auch die Endgeräte wie Computer, Laptops, Smartphones und Tablets vor Hacker-Angriffen geschützt werden. So sollte z. B. sichergestellt sein, dass alle Geräte mit den neuesten Sicherheitsupdates versehen sind – eine wichtige Maßnahme, um bekannte Schwachstellen zu schließen. Zusätzlich sollten starke Passwörter verwendet und Sicherheitssoftware installiert sein, um potenzielle Bedrohungen zu minimieren.

✓ **DDoS-Schutzmechanismen:** Bei einem sogenannten Distributed-Denial-of-Service-(DDoS-) Angriff wird versucht, ein Netzwerk oder eine Webseite durch eine massive Überlastung der Ressourcen außer Betrieb zu setzen. Eine Firewall schützt nicht vor DDoS-Attacken, da sie meist selbst das Ziel oder Teil des Problems ist. Daher sollten Unternehmen DDoS-Schutzmechanismen implementieren, die den eingehenden Datenverkehr überwachen, umfangreiche Aktivitäten erkennen und so darauf reagieren, dass ein reibungsloser Betrieb weiterhin gewährleistet ist.

»

Die Schulung und Sensibilisierung des Personals ist von entscheidender Bedeutung, um Phishing-Angriffe, Social Engineering und andere betrügerische Aktivitäten zu erkennen und zu verhindern.

«

✓ **Backups:** Eine zuverlässige Backup-Strategie ist entscheidend, um sich vor Datenverlust und den Auswirkungen von Cyberangriffen zu schützen. Regelmäßige Backups aller wichtigen Daten und Systeme stellen sicher, dass im Falle eines Ransomware-Angriffs, Hardware-Ausfalls oder anderer Katastrophen die Daten gespeichert werden können. Idealerweise sollten Backups an einem sicheren Ort aufbewahrt und regelmäßig getestet werden, um sicherzustellen, dass sie im Ernstfall effektiv funktionieren.

✓ **Patchmanagement:** Softwarehersteller veröffentlichen regelmäßig Patches und Updates, um Sicherheitslücken zu schließen und bekannte Schwachstellen zu beheben. Ein effektives Patchmanagement stellt sicher, dass alle Systeme und Software in einem Netzwerk auf dem neuesten Stand sind. Durch diese regelmäßige Aktualisierung können Unternehmen von den neuesten Sicherheitsverbesserungen profitieren und potenzielle Angriffspunkte minimieren.

✓ **Schwachstellen- oder Vulnerability-Management:** Neben dem Patchmanagement sorgt dies weiter für Sicherheit – es beinhaltet die kontinuierliche Überwachung von Netzwerken und Systemen auf neue Schwachstellen und die Bewertung ihres Risikos. Durch regelmäßige Schwachstellen-Scans können potenzielle Angriffsvektoren identifiziert und priorisiert werden, um proaktive Maßnahmen zur Risikominderung zu ergreifen. Die Kombination von effektivem Patchmanagement und umfassendem Vulnerability-Management ermöglicht es Unternehmen, ihre Sicherheitslage zu verbessern, ihre Angriffsfläche zu minimieren und potenzielle Sicherheitsverletzungen einzudämmen.

✓ **Faktor Mensch:** Mitarbeitende sind eine wichtiger Schutzwall in der Cybersicherheit. Deren Schulung und Sensibilisierung sind von entscheidender Bedeutung, um Phishing-Angriffe, Social Engineering und andere betrügerische Aktivitäten zu erkennen und zu verhindern. Unternehmen sollten regelmäßige Schulungen anbieten, die Mitarbeitende über aktuelle Bedrohungen aufklären und sie darin schulen, starke Passwörter zu verwenden, verdächtige E-Mails zu erkennen und sicher im Internet zu surfen. Denn die technischen Schutzvorkehrungen können noch so gut sein: Letztlich gilt der Mensch als die größte Sicherheitslücke. Nicht umsonst fordern Cybersecurity-Versicherungen als Grundvoraussetzung für den Vertragsabschluss regelmäßige unternehmensweite Security-Awareness-Schulungen.

5.3 Colocation: Externe Rechenzentren als Schutz vor physischen Bedrohungen

Der Tresor für Daten und Server
Wenn Unternehmen die Ausfallsicherheit ihrer Unternehmens-IT noch weiter erhöhen möchten, bietet sich eine Auslagerung von Servern und Daten in ein externes Rechenzentrum an. Diese schützen insbesondere vor physischen Bedrohungen wie Feuer, Hitze, Hochwasser, Vandalismus und unberechtigtem Zugriff.

Sie sind dort oft sicherer verwahrt als in den eigenen Serverräumen, denn gerade kleine und mittlere Unternehmen haben oft nicht die Ressourcen für einen umfassenden physischen Schutz oder eine redundante Stromversorgung.

Es hat noch weitere Vorteile, die Daten auch an einem anderen Ort als dem Firmenstandort zu speichern. Dank Klimatisierung haben die Server immer die richtigen Temperaturbedingungen. Und bei einem Brand im eigenen Serverraum oder bei Hochwasser gehen Daten nicht verloren.

Nähe bringt Geschwindigkeit
Befindet sich das Colocation-Rechenzentrum direkt am Backbone des Providers und zudem in der Region des Unternehmens, wirkt sich das positiv auf die Übertragungsraten aus. Einige Unternehmen lagern deshalb zum Beispiel ihre cloudbasierten Daten in ein Colocation-Rechenzentrum im Umkreis des Firmensitzes aus. Denn das beschleunigt die Verarbeitung und Speicherung der Daten. Außerdem ist sichergestellt, dass die Datenschutz-Grundverordnung (DSGVO) eingehalten wird.

Backup-Kopie sicherheitshalber auslagern
Wer sich vor Ransomware-Angriffen schützen möchte, kann eine Backup-Kopie seiner Daten zusätzlich auf einem vom Unternehmensnetz isolierten Server in einem Provider-Rechenzentrum speichern

Sechs gute Gründe für die IT-Auslagerung in ein Colocation-Rechenzentrum

- ✓ Highspeed-Anbindung
- ✓ Professioneller Brandschutz
- ✓ Zugangsregulierung
- ✓ Gesicherte Stromversorgung
- ✓ Konstante Klimabedingungen
- ✓ Hochverfügbare Technik

6. Fazit: Wie Unternehmen ihre IT-Umgebung nachhaltig absichern können

IT-Aufgaben einfach outsourcen
Die größten Risiken für Unternehmen lassen sich durch eine ausfallsicher konzipierte IT-Infrastruktur sowie mit Cybersecurity-Maßnahmen minimieren. Weder eine gekappte Internetanbindung noch ein Cyberangriff muss in die Insolvenz führen.

Da der Fachkräftemangel im IT-Bereich derzeit enorm ist, profitieren vor allem kleine und mittlere Unternehmen von ausgewählten Managed Services eines Netzanbieters. So kann selbst bei einem kleinen IT-Team eine sichere IT-Umgebung aufgebaut und nachhaltig betrieben werden.

Von Expertise des Managed Service Providers profitieren
Netzprovider müssen ihr eigenes Netz und ihre Rechenzentren als wichtige Versorgungsinfrastruktur immer auf dem neuesten Stand der Technik halten. Das gilt insbesondere für die IT-Security und Ausfallsicherheit. Über die Managed Services können Kundenunternehmen von dieser Expertise profitieren.

Angesichts ständig neuer Angriffsszenarien, aber auch sich laufend verändernder Unternehmensanwendungen und IT-Netze, ist solch eine Unterstützung eine gute Option. Denn dadurch ist gewährleistet, dass Infrastruktur oder Sicherheitsmaßnahmen stets auf dem neuesten Stand der Technik sind.

Mit zunehmender Digitalisierung wird die IT künftig einen noch größeren Stellenwert im Unternehmen einnehmen – und somit auch die Verfügbarkeit der IT-Infrastruktur mit ihren Anwendungen und Services. Ausfallsicherheit und Cybersicherheit werden also noch wichtiger werden, damit Geschäftsprozesse reibungslos und ohne Betriebsunterbrechungen ablaufen können.

Budget einplanen für IT-Sicherheit
Redundant ausgelegte Infrastrukturen und wirksame Cybersicherheitsmaßnahmen gibt es nicht zum Nulltarif. Selbst kleine und mittlere Unternehmen werden künftig in Sicherheit investieren und gegebenenfalls IT-Budgets dafür umschichten müssen.

7. Checkliste: Überprüfen Sie Ihre IT-Sicherheitsvorkehrungen

Welche Maßnahmen haben Sie schon ergriffen? Die wichtigsten Punkte, die Sie umsetzen sollten:

- ☐ Identifizieren Sie kritische und nicht-kritische Prozesse und Dienste in Ihrer Organisation.
- ☐ Stellen Sie sicher, dass Notfallpläne für kritische Prozesse vorhanden sind, um auf mögliche Störungen oder Ausfälle vorbereitet zu sein.
- ☐ Klären Sie, wer befugt ist, im Falle eines Sicherheitsvorfalls (auch unangenehme) Entscheidungen zu treffen.
- ☐ Legen Sie klare Meldefristen für Sicherheitsvorfälle fest, um eine rechtzeitige Reaktion und Behebung zu gewährleisten.
- ☐ Bestimmen Sie, wer die Verantwortung für die IT-Sicherheit in Ihrem Unternehmen trägt und wer im Falle eines Vorfalls handelt, indem Sie die notwendigen Rollen im Voraus definieren.
- ☐ Überprüfen Sie interne und externe Abhängigkeiten wie Schnittstellen zu Partnern, Warenwirtschaftssystemen, Heimarbeitsplätzen oder Cloud-Anwendungen.
- ☐ Evaluieren Sie, welche Redundanzen in Bezug auf Switches, Server, Datenverbindungen und Backup-Möglichkeiten erforderlich sind.
- ☐ Analysieren Sie die Konnektivität Ihrer Standorte und prüfen Sie Service Level Agreements (SLAs), Austauschzeiten für Endgeräte und Schutzmaßnahmen bei Leitungsausfällen.
- ☐ Überprüfen Sie die Sicherheit der Schnittstellen zum Internet und zur Cloud, einschließlich geeigneter Schutzmaßnahmen wie Passwortschutz, Zwei-Faktor-Authentifizierung, VPN und Zugriffsberechtigungen.
- ☐ Überprüfen Sie Schnittstellen und Komponenten regelmäßig auf potenzielle Schwachstellen.
- ☐ Stellen Sie sicher, dass angemessene Sicherheitsmechanismen wie Netzwerksicherheit (unter anderem Firewalls), Antiviren-/Endgeräteschutz, Zwei-Faktor-Authentifizierung, VPN, Zero-Trust-Prinzip, Berechtigungsmanagement und Incident Management vorhanden sind.
- ☐ Gewährleisten Sie eine kontinuierliche Sensibilisierung Ihrer Mitarbeiter für IT-Sicherheit.
- ☐ Definieren Sie eine Backup-Strategie zur Sicherung Ihrer Daten.
- ☐ Stellen Sie sicher, dass Ihre IT-Systeme regelmäßig aktualisiert werden und ausreichende IT-Ressourcen zur Verfügung stehen, um sie stets auf dem neuesten Stand zu halten.
- ☐ Sorgen Sie dafür, dass Ihre Server ausreichend gegen Vandalismus, Feuer, Hitze, Stromausfall oder Naturkatastrophen wie Hochwasser geschützt sind.
- ☐ Informieren Sie sich über die rechtlichen Anforderungen, die Ihre Organisation aufgrund von Richtlinien erfüllen muss (zum Beispiel NIS-Richtlinie für KRITIS-Unternehmen).

Über die EWE TEL GmbH

Die EWE TEL GmbH ist ein deutsches Telekommunikations- und IT-Unternehmen mit Hauptsitz im niedersächsischen Oldenburg. Das Unternehmen wurde im Jahr 1999 als hundertprozentige Tochtergesellschaft der EWE AG gegründet und bietet eine breite Palette an Telekommunikations- und IT-Dienstleistungen für Unternehmen, Institutionen und Privatkundschaft an. Hierzu gehören unter anderem Festnetz- und Mobilfunkdienste, Internet und Datendienste sowie IT- und Sicherheitslösungen. Dabei legt das Unternehmen besonderen Wert auf hohe Qualität und Verfügbarkeit seiner Dienstleistungen.

Die EWE TEL GmbH betreibt ein Glasfasernetz mit einer Länge von mehr als 40.000 Kilometern und ist somit einer der größten Netzbetreiber in Norddeutschland. Zudem betreibt das Unternehmen eigene Rechenzentren und verfügt über eine hochperformante Infrastruktur für seine Kundschaft.

Mit seinen innovativen Lösungen und seinem umfassenden Know-how in der Telekommunikations- und IT-Branche ist EWE TEL ein zuverlässiger Business-Partner für Unternehmen jeder Größe und Branche.

Umfassende ITK-Dienstleistungen für den Mittelstand im Nordwesten Deutschlands

Das Portfolio von EWE TEL umfasst neben Telefonie-, Internet- und Datenverbindungen auch Colocation-Dienste und Managed Security Services. Dazu zählen zum Beispiel Managed-Firewall-Services, DDoS-Schutz, Endpoint-Protection sowie Security-Awareness-Schulungen.
Hinzu kommen zahlreiche Infrastrukturdienstleistungen für Unternehmen – wie die Unterstützung bei der Konzeption und dem Betrieb von ausfallsicheren Internetanbindungen.

Darüber hinaus übernimmt EWE TEL als Service Provider auf Wunsch nicht nur die komplette Vernetzung der WAN-Verbindungen eines Unternehmens, sondern auch die für das LAN und WLAN. Zudem baut EWE TEL sein Glasfasernetz sowie das Managed-Service-Angebot kontinuierlich aus. Insbesondere der Mittelstand profitiert dabei vom kompetenten und schnellen Service vor Ort.

Kontakt

0800 1393835
business.ewe.de
business@ewe.de