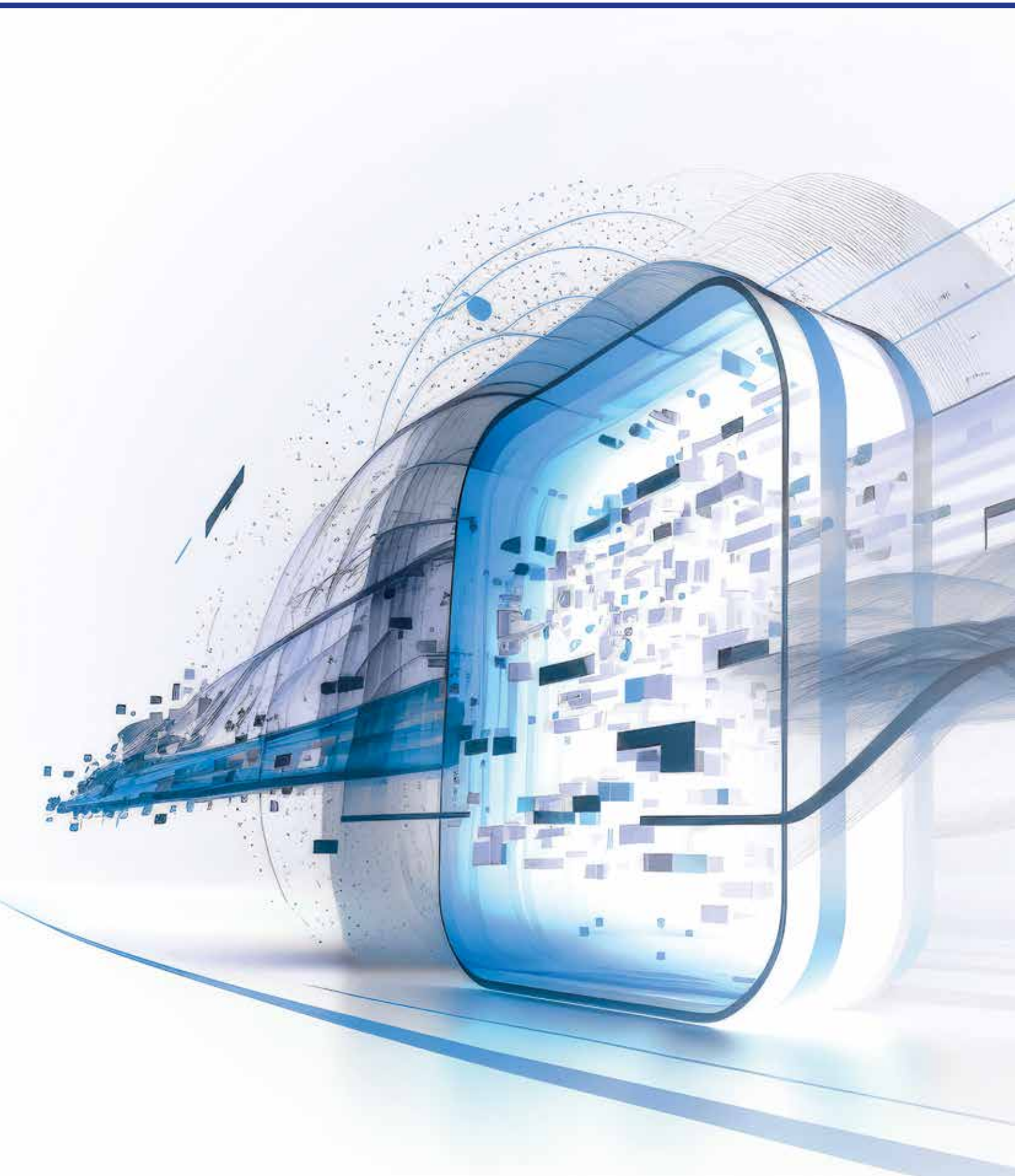
Schaal IT-Service

IT-SICHERHEIT

IHR UNTERNEHMEN RUNDUM GESCHÜTZT

www.schaal-it.de



INHALTSVERZEICHNIS

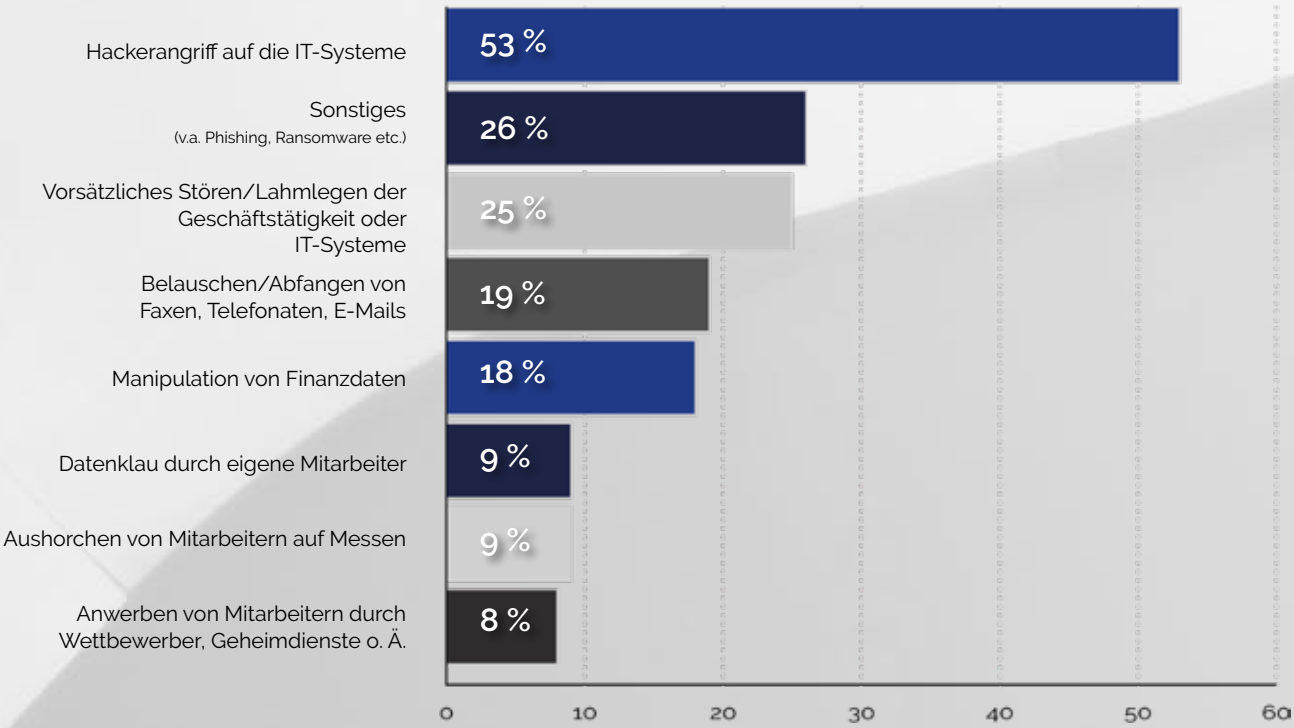
INFOGRAFIK

IT-SICHERHEIT

Eigene Einschätzung zum Cyberrisiko im Unternehmen 2023

EY. (16. Mai, 2023). Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen/Datenklau zu werden? [Graph]. In Statista. Zugriff am 03. Juni 2024, von https://de.statista.com/statistik/daten/studie/760006/umfrage/wahrgenommenes-risiko-von-cyberangriffen-unter-unternehmen-in-deutschland/

Art des Angriffs bei betroffenen Deutschen Unternehmen



EY. (16. Mai, 2023). Welche konkreten Handlungen fanden statt? [Graph]. In Statista. Zugriff am 03. Juni 2024, von https://de.statista.com/statistik/daten/studie/760303/umfrage/angriffsformen-von-cyberkriminalitaet-gegen-deutsche-unternehmen/

411.000
neue schädliche Dateien täglich
oder 5 Schädlinge pro Sekunde

125 Millionen
schädliche Dateien wurden im Jahr 2023
von Januar bis Oktober entdeckt

Anstieg der schädlichen Dateien im Vergleich zu 2022

267% Anstieg des Anteils von Backdoor-Trojanern

24.000 schädliche Dateien täglich

in Microsoft Office und anderen Dokumententypen

88% der täglich abgeschickten Schadprogramme

zielten auf Windows-Geräte ab

alle **39 Sekunden**

fand ein Cyberangriff statt, 2022 nur alle 44 Sekunden

Quelle: https://www.watchguard.com/de/wgrd-news/blog/im-jahr-2023-gab-es-alle-39-sekunden-einen-cyberangriff

Quelle: https://www.kaspersky.de/blog/kaspersky-rueckblick-2023/30731/#:~:text=Kaspersky%2DL%C3%B6sungen%20haben%20in%20diesem,drei%20Prozent%20gegen%C3%BCber%20dem%20Vorjahr.

Gut zu wissen:

40% Anstieg der Phishing-Link-Zugriffsversuchen

Um eine möglichst große Erfolgsquote zu haben, richten sich die Cyberkriminellen mit ihren Phishing-Attacken nicht an bestimmte Unternehmen, sondern versuchen einfach, so viele Sicherheitslücken wie möglich auszunutzen. Deshalb kann jedes Unternehmen, egal welcher Größe, ohne die nötigen IT-Sicherheitsvorkehrungen zum Opfer werden.

Quelle: https://www.itsicherheit-online.com/news/cybersecurity/report-phishing-aktivitaeten-steigen-weltweit-um-40-prozent/

HACKERANGRIFFE BEISPIELE

Beispiele von Unternehmen, die bereits einen Hackerangriff erlitten

Motel One

Ende September 2023

Art: Professioneller Angriff

Schaden: Millionen Namen, Adressen und Reisedaten von Gästen wurden von der Hackergruppe ALPHV (Blackcat) gestohlen und im Darknet veröffentlicht.

Quelle aller Angaben:

https://www.chip.de/news/Sind-Sie-betroffen-Die-5-heftigsten-Hacker-angriffe-in-Deutschland-2023_185110063.html

IHK

03. August 2022

Art: Professioneller Angriff

Schaden: In unterschiedlicher Form waren alle 79 IT-Systeme der IHK betroffen. Teilweise funktionierte E-Mail- und Telefonverkehr sowie interne Software-Anwendungen nicht mehr.

Es dauerte Wochen, um sicher wieder alles in Betrieb zu nehmen.

Quelle: https://www.ihk.de/bodensee-oberschwaben/servicemarken/presse/aktuelle-meldungen/pressemeldungen2022/update-zum-cyberangriff-auf-die-ihk-5627672

Baustoffhersteller Knauf

30. Juni 2022

Art: Ransomware

Schaden: 500GB großes Datenpaket mit Passwörtern, Kopien von Ausweis und Kreditkarten etc.

Quelle: https://www.inside-it.ch/3-wochen-nach-cyberangriff-hat-der-baustoffriese-knauf-immer-noch-probleme-20220721

Wieso sollten gerade kleinere Unternehmen ihren Sicherheitsstandard erhöhen?

Da viele Cyberangriffe nicht gezielt ein Unternehmen angreifen, sondern gesammelt versuchen bei so vielen IT-Systemen wie möglich Schwachstellen auszunutzen, sind gerade kleinere Unternehmen meist angreifbarer als große Firmen mit einem ausgereiften Sicherheitssystem.

Ein Grund für häufigere Angriffe :

CaaS

Cybercrime as a Service

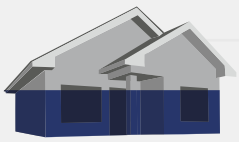
Was heißt Cybercrime as a Service?

Ähnlich wie auch legale Softwareentwickler für einen bestimmten Preis ihre Software zur Verfügung stellen, gibt es mittlerweile auch ein illegales Geschäftsmodell für Schadsoftware. Dieses wird immer mehr publik, weil es somit auch Kriminellen ohne Programmierkenntnisse o. Ä.. möglich wird, schädliche Cyberangriffe zu starten.

Mindestens ein Mal von einer Cyberattacke betroffene Unternehmen laut einer HDI-Cyber-Studie

36 %

der Kleinstunternehmen mit bis zu 9 Mitarbeitern

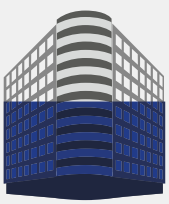


45 %

der Kleinunternehmen mit 10-49 Mitarbeitern

52 %

der Mittelständler mit 50-249 Mitarbeitern



Quelle: https://services.hiscox.de/wp-content/uploads/2023/10/Hiscox-Cyber-Readiness-Report-2023-Infografik_1.pdfhttps://www.verkehrsrundschau.de/nachrichten/recht-geld/hdi-cyber-studie-erhebliche-schaeden-durch-angriffe-moeglich-3162406

CYBER-RESILIENZ

Was ist Cyber-Resilienz?

Cyber-Resilienz bedeutet die Widerstandsfähigkeit, die ein Unternehmen gegen Sicherheitsvorfälle und Cyberangriffe. Ein gutes Cyber-Resilienzprogramm sorgt dafür, die täglichen Sicherheitsherausforderungen zu meistern und die Auswirkungen eines Cyberangriffes zu minimieren.

Somit wird der Bestand des Unternehmens gesichert und Verluste durch Cyberangriffe reduziert.

Was ist der Unterschied zur Cybersicherheit?

Cybersicherheit konzentriert sich auf den Schutz von digitalen Vermögenswerten vor Cyberangriffen wie z.B. Ransomware oder Malware.

Cyber-Resilienz dagegen, man könnte auch Sicherheitsstrategie sagen, ist die Fähigkeit eines Unternehmens, Schäden und Verluste zu verhindern und gleichzeitig einen schnellen und effizienten Wiederaufbau im Falle eines Cyberangriffs zu ermöglichen.

Vorteile einer Cyber-Resilienz

Schnelle Wiederherstellungszeit, höhere Produktivität und Effizienz

...durch weniger Ausfallzeiten und Serviceunterbrechungen.

Verbesserter Schutz vor Cyber-Bedrohungen und -Angriffen

Der Aufbau einer Cyber-Resilienzstrategie stärkt die Cyber-Sicherheitstools und -Praktiken um zukünftige Angriffe zu erschweren.

Einhaltung gesetzlicher und branchenspezifischer Vorschriften

... wie DSGVO oder GoBD.

Schützt den Unternehmensruf und stärkt das Vertrauen der Kunden

Verbessert die allgemeine Sicherheitslage und Notfallswiederherstellung

Reduzierung finanzieller Verluste

Praktiken zum Aufbau einer Cyber-Resilienz-Strategie

Bereitstellung eines wirksamen Sicherheitssystems

Zum Schutz der gesamten IT-Infrastruktur, aller Systeme, Benutzer und Daten.

Regelmäßige Backups

Zum Schutz der aktuellen Daten, damit diese im Falle eines Verstoßes oder Kompromittierung wiederhergestellt werden können.

Erstellung und Umsetzung eines zuverlässigen Business-Continuity und Disaster-Recovery-Plans (BCDR)

Plan zum Krisenmanagement, Mitarbeitersicherheit und alternative Arbeitsorte

Post-Angriffsanalyse

Hilft dabei, Sicherheitslücken zu schließen um besser auf zukünftige Bedrohungen reagieren zu können.

ZERO-TRUST-MODELL

Was ist ein Zero-Trust-Modell?

Das Zero-Trust-Modell („Null-Vertrauen-Modell“) ist ein Sicherheitskonzept, das auf dem Grundsatz basiert, keinem Gerät, Nutzer oder Dienst innerhalb und außerhalb des eigenen Netzwerks zu vertrauen.

Daraus resultiert die Forderung, sämtliche Anwender zu authentifizieren und den Datenverkehr grundsätzlich zu verschlüsseln.

Mit Home-Office und standortunabhängigem Arbeiten wird das Zero-Trust-Modell zum effizienten Schutz des Firmennetzwerks immer wichtiger.

HERKÖMMLICHE SICHERHEITSMODELLE

Herkömmliche Sicherheitsmodelle gehen davon aus, dass alle Dienste, Geräte und Anwender innerhalb des eigenen Netzwerks vertrauenswürdig sind.

Nur Netzwerkverkehr und Zugriffe von außen werden als potenziell gefährlich eingestuft und analysiert.

NACHTEIL

Sobald ein Schädling erfolgreich ins Firmennetz eingedrungen ist, gibt es kaum noch Sicherheitsvorkehrungen, die ihn stoppen.

VERTRAUENS-WÜRDIGKEIT DES NETZWERKS

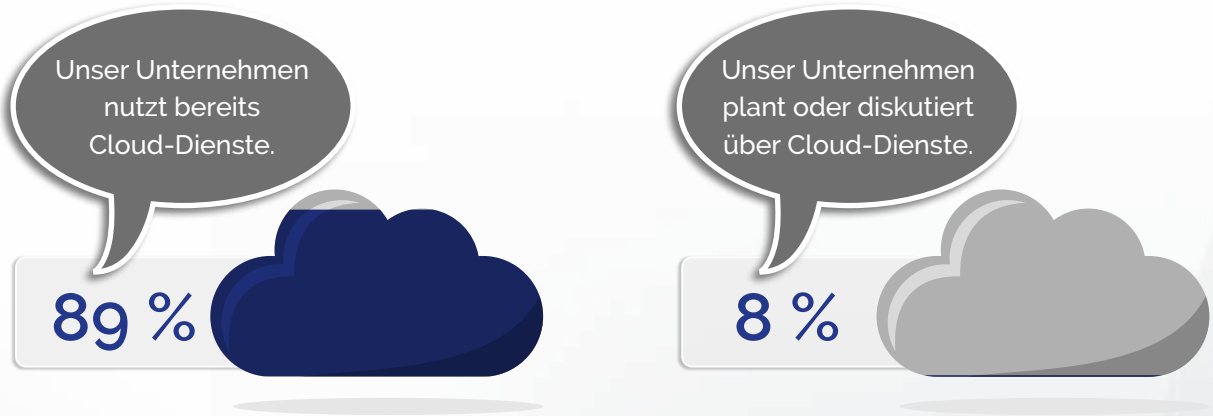
Durch das Zero-Trust-Modell kann die Sicherheit Ihres Unternehmens verbessert und gleichzeitig das Risiko von Malware verringert werden. Nutzer und Geräte stellen dadurch standortunabhängig eine sichere Verbindung zum Internet her. Gleichzeitig wird das System proaktiv auf Bedrohungen geprüft.

SICHERER ANWENDERZUGRIFF FÜR MITARBEITER UND PARTNER

Herkömmliche Zugriffstechnologien wie VPN basieren auf veralteten Prinzipien und können gerade bei geklauten Nutzerdaten dazu führen, dass sich ein Schädling ebenfalls Zugriff verschafft. Durch Zero-Trust-Sicherheit werden detaillierte Sicherheitsrichtlinien festgelegt.

SICHERE UMGEBUNG IN DER CLOUD

Nutzung von Cloud-Diensten durch Deutsche Firmen 2023



Quelle: Deutschland; KPMG; Bitkom Research; 2022: 552 Unternehmen; Geschäftsführer und IT-Führungskräfte aus Unternehmen ab 20 Mitarbeitern

Vorteile einer integrierten Cloud-Umgebung

Bessere Performance und erhöhte Datenverfügbarkeit

Verfügbarkeit und Wartung der IT-Ressourcen werden 24/7 sichergestellt. Außerdem sind neue Anwendungen und ihre Funktionalität sofort verfügbar.

Einhaltung der deutschen Sicherheitsstandards

Da wir die Daten verschlüsselt in einem deutschen Rechenzentrum aufbewahren, sind auch diese an die deutschen Sicherheitsvorschriften gebunden.

Schutz vor Katastrophen

Die Rechenzentren, in denen die Daten liegen sind bestens mit Notstromversorgung und redundanten Servern auf Katastrophen und Ausfälle vorbereitet.

Standortunabhängiges Arbeiten

Durch eine virtuell aufgebaute Arbeitsumgebung, können alle Mitarbeiter unabhängig von Standort und Endgerät darauf zugreifen.

Der Umzug in die Cloud bedeutet aber auch veränderte Sicherheitsstrukturen

Dank der vielen Vorteile, die eine integrierte Cloud-Umgebung bietet, ist sie in fast keinem Unternehmen mehr wegzudenken. Doch wie bei allem, bietet mehr Komfort auch mehr Sicherheitsrisiken.

Um diesen entgegenzuwirken, haben auch wir unsere Sicherheitsstrukturen angepasst und neue Features, mit denen wir auch in Zukunft ihre Daten lokal und in der Cloud sicher schützen können.

MFA
(Multi-Faktor-Authentifizierung)

Bei der MFA muss der Benutzer zwei oder mehrere Verifizierungsfaktoren angeben, um Zugang zu seinem Konto zu bekommen. Somit ist es Cyberkriminellen immer schwieriger möglich, sich als den verifizierten Nutzer auszugeben.

Die wichtigsten Möglichkeiten der MFA:

- Microsoft Authentificator-App
  (generiert zeitlich berenzte Codes als MFA)
- Microsoft Hello for Business
  (Fingerprint, Pin oder Gesichtserkennung)
- OTP-Token | Physischer Schlüssel
  (externer Schlüssel zur MFA)
- Conditional Access
  (Bedingter Zugriff)

DOKUMENTATIONSSYSTEM

IT Glue

IT Glue ist ein Dokumentationssystem, das die Daten verschlüsselt, und nur für Befugte zugänglich, in einem deutschen Rechenzentrum speichert.

MICROSOFT COMPANY BRANDING

Microsoft 365

Wir können Ihnen bei Ihrer Microsoft 365 Anmeldefläche ein Unternehmensbranding hinterlegen. Das bedeutet, dass wir Ihr Firmenlogo und Farbbranding hinterlegen. Dies ist ein zusätzlicher Schutz, damit Sie sicher sein können, dass die Anmeldeseite, egal von welchem Standort aus auch keine Fakeseite darstellt.

MICROSOFT BITLOCKER

Bitlocker ist eine Sicherheitsfunktion von Microsoft, die Ihre Systemlaufwerke, Festplatten verschlüsselt. Ohne den Schlüssel sind die Daten nicht lesbar, weshalb auch nach entfernen der Festplatte der Zugriff für Unbefugte blockiert wird.

Zum Beispiel haben Diebe keinen Zugriff auf die Firmendaten, auch wenn ein Firmennotebook gestohlen wurde.

MEHR SICHERHEIT FÜR IHRE E-MAILS

E-MAILS RISIKOFAKTOR NUMMER EINS

E-Mails sind nach wie vor die bevorzugte Angriffsmethode der Cyberkriminellen. Dabei werden die E-Mails und getarnten Fake-Websites immer professioneller und dadurch schlechter zu entlarven.

Um sich dabei nicht nur auf aufmerksame Mitarbeiter verlassen zu müssen, gibt es neue, sichere Möglichkeiten, um Sicherheitslücken im Bereich E-Mails besser zu schließen.

SPF, DKIM UND DMARC

Dies sind die drei wichtigsten E-Mail-Authentifizierungsprotokolle, die nachweisen, dass der Absender berechtigt ist, E-Mails im Namen einer Domain zu versenden.

Mithilfe dieser Sicherheitsabfragen, die alle im Hintergrund laufen, verringern Sie die Gefahr erheblich, dass Spam-Mails in Ihrem Namen verschickt werden oder Anhänge verändert wurden und damit schädliche Inhalte für dem Empfänger enthalten.

SPF
Sender Policy Framework

In SPF werden die E-Mail-Server festgelegt, von denen aus im Namen Ihrer Domain gesendet werden darf.

Der Empfänger-Server fragt daher zuerst ab, ob die E-Mail mit der Domain überhaupt von einem der im SPF stehenden Server gesendet wurde. Trifft dies nicht zu, kann sie als verdächtig angesehen werden.

DKIM
DomainKeys Identified Mail

DKIM ist ein eindeutiger digitaler Schlüssel, den Ihr E-Mail-Server vor dem versenden einer E-Mail generiert. Der Empfänger-Server überprüft, ob der Schlüssel vom Absender-Server mit dem der E-Mail übereinstimmt.

Ist der digitale Schlüssel identisch bedeutet das, dass die E-Mail und ihre Anhänge nicht manipuliert wurden und vertrauenswürdig ist.

DMARC
Domain-based Message Authentication, Reporting and Conformance

Die Aufgabe von DMARC ist es, die Schutzmaßnahmen zu koordinieren und Berichterstattung zu ermöglichen.

Mit DMARC wird festgelegt, was passiert, wenn eine E-Mail nicht vertrauenswürdig ist. Je nach Befehl wird diese dem Empfänger nicht zugestellt oder landet im SPAM-Ordner.

SICHERE LINKS

Zusätzlich zur regulären Anti-Spam- und Anti-Malware-Software wird jeder Link von Microsoft auf Sicherheitslücken geprüft, bevor Sie ihn öffnen können.

Prüfung von QR-Codes
Wird oft bei Phishing verwendet

Prüft URLs und Links in E-Mails
Zusätzlich zu Anti-Spam und Anti-Malware-Schutz

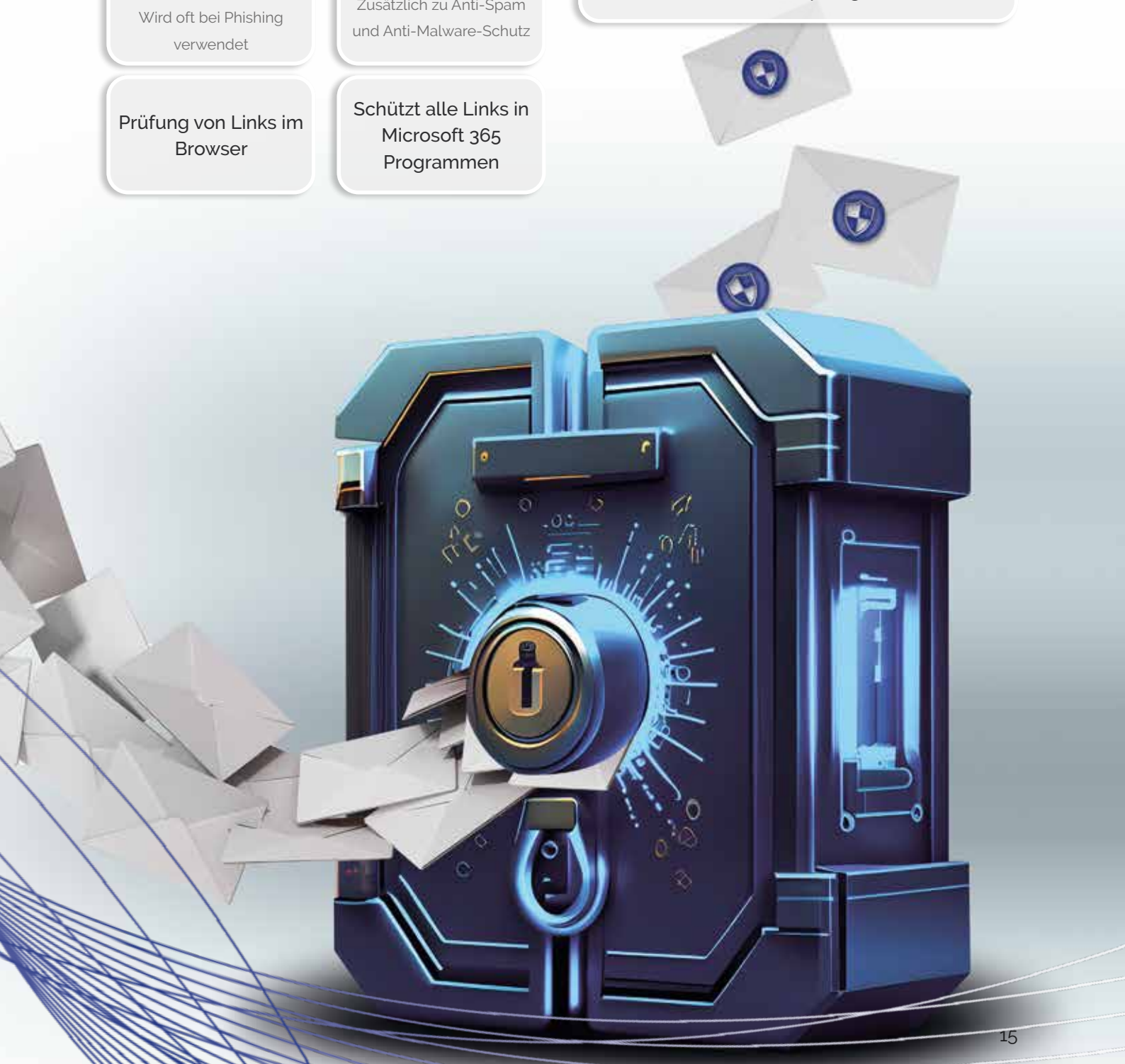
Prüfung von Links im Browser

Schützt alle Links in Microsoft 365 Programmen

SICHERE ANHÄNGE

Mit Microsoft 365 bzw. Outlook erhalten Sie eine zusätzliche Schutzebene, die dafür sorgt, dass Ihre E-Mail-Anlagen auf Sicherheit geprüft werden.

Prüfung der Anhänge für alle E-Mail-Empfänger



BACKUP-STRATEGIE

IHRE DATEN BESTMÖGLICH GESCHÜTZT

Die Datensicherung, oder auch Backup genannt, ist die effizienteste Möglichkeit, um wichtige und sensible Daten bestmöglich zu schützen.

Dabei können die Daten auf einem externen, lokalen Datenträger, oder über die Cloud in einem Rechenzentrum gespeichert werden. Beide Möglichkeiten haben ihre Vorteile, weshalb es Sinn macht, eine Strategie aus beiden zu entwickeln. Wir möchten Ihnen auf dieser Seite unsere Backup-Strategie vorstellen.

Diese Fragen sollten Sie sich beantworten

RPO und RTO?

RPO (Recovery Point Objective)

In welchen Abständen läuft die Datensicherung?
Wie viel Datenverlust ist tolerierbar?

RTO (Recovery Time Objective)

Wie schnell muss eine Anwendung nach Ausfall wieder verfügbar sein?
Wie schnell muss alles wieder einsatzbereit sein?

Vorteile eines lokalen Backups

Schnelle Wiederherstellung großer Datenmengen

Da das lokale Backup nicht von einer Internetverbindung abhängig ist, können große Datenmengen schnell wiederhergestellt werden.

Volle Kontrolle über das Backup

Da das Backup lokal auf einer NAS in Ihrem Unternehmen liegt, wissen Sie genau, wo Ihre Daten liegen.

Hohe Datensicherheit

Ein NAS-Backup vor Ort kann bei richtiger Einrichtung besonders sicher sein, da es in einem anderen Netzwerk eingebunden ist, als z.B. die PCs.

Weniger Kosten

Die Hardware für das Backup ist abgesehen von Verschleiß und Wartung eine einmalige Investition.

Vorteile eines Cloud-Backups

Flexible Skalierbarkeit

Der Cloud-Speicher kann je nach Speicherkapazität erweitert oder verringert werden.

Geografische Redundanz

Ihre Daten werden in zwei deutschen Rechenzentren (Hüllhorst und Düsseldorf) redundant gesichert. Dadurch sind Ihre Daten auch vor lokalen Katastrophen geschützt.

Erkennung von Ransomware

Wenn Ransomware auf dem Backup zu erkennen ist, lässt sich zurückverfolgen bis zu welchem Zeitpunkt das Backup intakt war. Aus diesem können Dateien wiederhergestellt werden.

Standortunabhäniger Zugriff

Durch die Vernetzung mit dem Internet, können die Daten von jedem Ort aus wiederhergestellt werden.

Disaster Recovery Test | Backup-Validierung

Wir können Ihr Backup regelmäßig auf die Funktionsfähigkeit überprüfen, um sicher zu gehen, dass das Zurückspielen im Ernstfall auch wirklich funktioniert.

UNSERE STRATEGIE
Multi-Vendor-Strategie

Beide Backup-Möglichkeiten haben ihre Vorteile, weshalb wir auf eine Multi-Vendor-Strategie setzten. Das bedeutet, dass wir Ihre Daten sowohl lokal, als auch in der Cloud, mit zwei Verschiedenen Anbietern sichern.

Redundanz und Ausfallsicherheit

Ihre Daten sind an verschiedenen Standorten und auf unterschiedlichen Systemen gesichert. Somit haben sie eine erhöhte Ausfallsicherheit.

Auch wenn das Internet oder ein Anbieter ein Problem hat, haben Sie immer noch die Möglichkeit auf das andere System zuzugreifen.

Höherer Schutz vor Sicherheitslücken

Jeder Anbieter hat eine andere Sicherheitsstrategie. Mit der Multi-Vendor-Strategie stellen wir sicher, dass Ihre Daten gegen möglichst viele und unterschiedliche Sicherheitslücken geschützt sind.

MONITORING UND WARTUNG

ÜBERWACHUNG UND AKTUALISIERUNG DES KOMPLETTEN SYSTEMS

Neben den Sicherheitsmaßnahmen für spezifische Bereiche Ihres Systems, ist es eben so wichtig das komplette System zu überwachen und zu warten. Die verschiedenen Anbieter bieten regelmäßig neue Updates, die Sicherheitslücken schließen.

Außerdem kann das Monitoring dabei helfen, frühzeitig Probleme im System zu erkennen. Das verkürzt die Ausfallzeit und Fehlersuche.

MONITORING

Monitoring bzw. System Monitoring bedeutet, dass wir als IT-Verantwortliche Ihre IT-Infrastruktur dauerhaft überwachen. Dazu zählen zum Beispiel Festplattenspeicherplatz und Belegung. Aber auch Anwendungen etc. können werden überwacht.

Zusammengefasst werden alle wichtigen Geräte Ihrer IT-Infrastruktur dauerhaft auf Verfügbarkeit und Performance geprüft.

WARTUNG

Die Wartung Ihres Systems sorgt dafür, dass es auf dem aktuellen Stand bleibt und bestmöglich gegen Sicherheitslücken geschützt ist.

Frühzeitige Erkennung von Problemen

Durch die dauerhafte Überwachung Ihrer IT-Infrastruktur können schon frühzeitig Probleme erkannt werden (z.B. Backup nicht durchgeführt).

Dadurch lassen sich gravierende Ausfälle vermeiden bzw. schnelle Wiederherstellungsverfahren einleiten.

Schutz der Firmendaten

Das Monitoring beschränkt sich auf die Überwachung der IT-Infrastruktur, weshalb die Software **KEINEN** Einblick in Ihre vertraulichen Daten bietet.

Identifizierung von Schwachstellen

Regelmäßige Updates sorgen dafür, dass bekannte Sicherheitslücken geschlossen werden, bevor Angreifer sich diese zu nutzen machen können.

KONTAKT

Schaal IT-Service GmbH

Kohlmattstraße 7
D - 77876 Kappelrodeck

+49 (0) 7842 45 99 600
+49 (0) 7842 45 99 699

service@schaal-it.de
www.schaal-it.de