MEHR WISSEN. DAS THEMEN-DOSSIER VOM ERFOLG MAGAZIN

ERFOLG magazin

DOSSIER

\+ 10 TIPPS, UM SICH VOR CYBERANGRIFFEN ZU SCHÜTZEN

EXPERTE IN DIESER AUSGABE

REHAN KHAN

CYBER SICHERHEIT:

»Kein System ist **unangreifbar**!«

E-PAPER AUSGABE 36 · 2025

DEUTSCHLAND | ÖSTERREICH | SCHWEIZ

Bild: Rene Schmitt

INHALT

Impressum

Folgen Sie uns auch auf

ERFOLG Magazin Dossier

Redaktion/Verlag
Backhaus Verlag GmbH
ist ein Unternehmen der Backhaus Mediengruppe
Holding GmbH, Geschäftsführender
Gesellschafter Julien Backhaus

E-Mail: info@backhausverlag.de
Chefredakteur (V. i. S. d. P.) Julien Backhaus
Redaktion: Anna Seifert, Martina Karaczko
E-Mail: redaktion@backhausverlag.de
Objektleitung: Judith Iben
Layout und Gestaltung: Christina Meyer, Judith Iben
E-Mail: magazine@backhausverlag.de

Onlineredaktion
E-Mail: info@backhausverlag.de

Herausgeber, Verleger:
Julien Backhaus

Anschrift
Zum Flugplatz 44
27356 Rotenburg
Telefon (0 42 68) 9 53 04 91
E-Mail: info@backhausverlag.de
Internet: www.backhausverlag.de

Autoren (V. i. S. d. P.)
Die Autoren der Artikel und Kommentare im ERFOLG Magazin sind im Sinne des Presserechts selbstverantwortlich. Die Meinung der Autoren spiegelt nicht unbedingt die Meinung der Redaktion wider. Trotz sorgfältiger Prüfung durch die Redaktion wird in keiner Weise Haftung für Richtigkeit geschweige denn für Empfehlungen übernommen. Für den Inhalt der Anzeigen sind die Unternehmen verantwortlich.

Julien Backhaus
Verleger und
Herausgeber

Bild: Daniela Schenk

CYBERANGRIFFE LAUERN ÜBERALL: WARUM IT-SICHERHEIT CHEFSACHE IST

Oft braucht es nur einen Klick – vielleicht war es eine Phishing-Mail, die unbedacht geöffnet wurde, eine kleine Sicherheitslücke oder ein ungesichertes Passwort – und plötzlich sind die Server blockiert, die Systeme lahmgelegt und die Kundendaten gestohlen. Die Folgen? Hohe finanzielle Verluste, massive Reputationsschäden und im schlimmsten Fall der Stillstand des gesamten Unternehmens. In einer zunehmend digitalisierten Welt, in der Unternehmen immer stärker auf Cloud-Dienste, vernetzte Infrastrukturen und datenbasierte Geschäftsmodelle setzen, wächst die Angriffsfläche für Cyberkriminelle stetig.

Allein im dritten Quartal des Jahres 2024 wurden wöchentlich rund 1220 Cyberangriffe pro Unternehmen in Deutschland registriert – eine alarmierende Zahl, die verdeutlicht, dass Cybersicherheit längst zu einem der drängendsten Themen unserer Zeit geworden ist. Denn ein erfolgreicher Angriff kann nicht nur finanzielle Verluste verursachen, sondern auch das Vertrauen von Kunden und Geschäftspartnern nachhaltig erschüttern. Oftmals dauert es Wochen oder sogar Monate, bis sich ein Unternehmen von einem schweren Cyberangriff erholt – wenn es überhaupt gelingt. Doch trotz dieser Bedrohung handeln viele erst, wenn es bereits zu spät ist. Rehan Khan warnt eindringlich vor einer solchen Nachlässigkeit.

Der erfahrene IT-Dienstleister und CEO von Rabb IT Solutions und »IT Solutions Entrepreneur of the Year 2023« weiß, dass jeder Mitarbeiter ein potenzielles Einfallstor für Cyberkriminelle sein kann. Sicherheitsstrategien müssten daher auf allen Ebenen eines Unternehmens implementiert werden – sie allein der IT-Abteilung zu überlassen, wäre fahrlässig. Wir freuen uns, Rehan Khan für dieses Dossier gewonnen zu haben. Dank seines umfangreichen Wissens und seiner langjährigen Erfahrung, mit der er wertvolle Einblicke in die Welt der IT-Sicherheit bietet, können wir uns keinen besseren Experten vorstellen als ihn.

Viel Vergnügen beim Lesen
Ihr Julien Backhaus

Cybersicherheit:

»Kein System ist unangreifbar!«

Von raffinierten Hackergruppen über Erpressungstrojaner bis hin zu unsichtbaren Schwachstellen in der IT: Cybersicherheit ist für Unternehmen längst zur Notwendigkeit geworden. Aber obwohl die Angriffe immer professioneller werden, hinken Unternehmen oft hinterher. Doch welche Einfallstore bieten sich Datendieben und welche Branchen sind besonders gefährdet? Diese Fragen stehen im Fokus unseres Gesprächs mit dem IT-Experten Rehan Khan. Wie man Cyberbomben am besten entschärft und wann es die Unterstützung eines IT-Dienstleisters braucht, hat uns der CEO von Rabb IT Solutions erklärt.

Herr Khan, das Thema Cybersicherheit im Unternehmensbereich wird immer relevanter, denn weltweit hat die Zahl der Cyberangriffe zugenommen. Aber woran liegt das eigentlich? Welche Branchen sind von den Attacken besonders betroffen?
Das ist absolut richtig – Cyberangriffe sind längst kein Hobby mehr, sondern ein hochprofitables Geschäftsfeld für organisierte Gruppen. Der Anstieg dieser Attacken hat mehrere Gründe. Einer der Hauptfaktoren ist die Digitalisierung und das hybride Arbeiten selbst: Unternehmen verlagern immer mehr Prozesse in die Cloud, nutzen vernetzte Geräte und setzen auf datengetriebene Geschäftsmodelle. Dadurch entstehen immer größere Angriffsflächen. Zudem hat die Professionalisierung im Bereich der Cyberkriminalität enorm zugenommen; Ransomware-as-a-Service ist ein Beispiel. Was die betroffenen Branchen angeht, gibt es heute keine klaren Grenzen mehr. Natürlich sind klassische Zielbranchen wie das Finanzwesen, das Gesundheitswesen und der öffentliche Sektor nach wie vor besonders im Fokus, da sie mit hochsensiblen Daten arbeiten. Aber auch produzierende Unternehmen, Logistikdienstleister und sogar mittelständische Betriebe sind zunehmend betroffen – insbesondere dann, wenn sie Zulieferer größerer Konzerne sind. Cyberkriminelle suchen gezielt nach den schwächsten Gliedern in der Lieferkette, um über diesen Zugang zu größeren Systemen zu erhalten.

An welchen Anzeichen lässt sich erkennen, ob die Sicherheit des eigenen Unternehmens gefährdet ist – und was können die Konsequenzen eines Cyberangriffs sein?
Ungewöhnliche Systemaktivitäten können ein erstes Warnsignal für einen Cyberangriff sein. Wenn Computer plötzlich langsamer laufen, Programme ohne erkennbaren Grund abstürzen oder im Hintergrund unbekannte Prozesse aktiv sind, sollten Mitarbeiter aufmerksam werden und die IT einschalten. Ebenso können unerwartete Zugriffsversuche ein deutliches Anzeichen sein. Ein weiteres Indiz ist ungewöhnliche E-Mail-Kommunikation.

Auch veränderte oder verschwundene Daten können auf eine Manipulation durch Angreifer hindeuten. Betriebsunterbrechungen sind eine der gravierendsten Auswirkungen, insbesondere wenn Systeme durch Ransomware verschlüsselt oder komplett lahmgelegt werden. In vielen Fällen kann dies den gesamten Geschäftsbetrieb stilllegen und enorme wirtschaftliche Schäden verursachen. Neben den finanziellen Einbußen durch Produktionsausfälle entstehen zudem hohe Kosten für die Wiederherstellung der Systeme, Maßnahmen zur Schadensbegrenzung und mögliche rechtliche Auseinandersetzungen – insbesondere dann, wenn Lösegeldforderungen im Raum stehen. Ein Cyberangriff kann auch erheblichen Reputationsverlust nach sich ziehen. Kunden und Geschäftspartner verlieren das Vertrauen in ein Unternehmen, wenn sensible Daten gestohlen oder sogar veröffentlicht werden – und natürlich sind auch rechtliche Konsequenzen nicht zu unterschätzen!

Kann es eine 100-prozentige Cybersicherheit überhaupt geben oder ist das eine Illusion? Welche Maßnahmen können Unternehmer ergreifen, um Risiken bestmöglich zu minimieren?
Nein, eine 100-prozentige Cybersicherheit ist eine Illusion. Kein System ist

vollkommen unangreifbar – selbst große Konzerne mit hochentwickelten Sicherheitsarchitekturen werden Ziel von Cyberattacken. Doch genau deshalb müssen Unternehmen IT-Sicherheit als strategische Priorität betrachten. Die Kunst liegt nicht darin, absolute Sicherheit zu erreichen, sondern die Hürden so hochzusetzen, dass Angriffe entweder frühzeitig erkannt oder für Cyberkriminelle unattraktiv werden.

Wie können Unternehmer Risiken bestmöglich minimieren?
Ein umfassender Schutz vor Cyberangriffen erfordert eine Kombination aus technischen Maßnahmen, geschulten Mitarbeitern, klaren Notfallplänen und einer geeigneten Absicherung. Ein wichtiger Bestandteil der IT-Sicherheit ist der Zero-Trust-Ansatz, bei dem sich jedes Gerät und jeder Nutzer kontinuierlich authentifizieren muss. Dadurch wird das Risiko minimiert, dass sich Unbefugte unerkannt in das Unternehmensnetzwerk einschleusen.

Neben technischen Schutzmaßnahmen spielt auch die Sensibilisierung der Mitarbeiter eine entscheidende Rolle. Da über 90 Prozent der Cyberangriffe mit einer manipulierten E-Mail beginnen, sind regelmäßige Phishing-Tests und Schulungen essenziell. Genauso wichtig sind klare Notfallpläne und regelmäßige Tests. Ein gut durchdachter Incident-Response-Plan sorgt dafür, dass im Ernstfall klare Abläufe definiert sind, um Schäden zu minimieren und schnell auf Sicherheitsvorfälle zu reagieren. Zusätzlich sollten Unternehmen auf eine Cyber-Versicherung setzen. Diese bieten Schutz vor den wirtschaftlichen Folgen eines Cyberangriffs und helfen, entstandene Schäden zu kompensieren. Durch eine Kombination aus diesen Maßnahmen lässt sich die IT-Sicherheit eines Unternehmens effektiv stärken und das Risiko eines erfolgreichen Angriffs erheblich reduzieren.

Wann ist es ratsam, einen IT-Dienstleister hinzuzuziehen und welche Faktoren zeichnen einen seriösen Anbieter aus?
Wenn die Komplexität der IT-Infrastruktur steigt, oder regulatorische Anforderungen erfüllt werden müssen, ist es ratsam, einen Experten hinzuzuziehen. Natürlich sollte auch an einen IT-Dienstleister gedacht werden, wenn es bereits Sicherheitsvorfälle oder Warnzeichen gab oder wenn internes Know-how fehlt.

Erfahrung und Referenzen sind ein entscheidendes Kriterium bei der Auswahl des IT-Dienstleisters. Unternehmen sollten prüfen, ob der Anbieter bereits erfolgreich Kunden ähnlicher Größe oder Branche betreut hat. Zertifizierungen und Standards

»Die Kunst liegt nicht darin, absolute Sicherheit zu erreichen, sondern die Hürden so hochzusetzen, dass Angriffe entweder frühzeitig erkannt oder für Cyberkriminelle unattraktiv werden.«
– Rehan Khan

sind dabei ein Qualitätsmerkmal, das für eine hohe Kompetenz spricht. Ein guter IT-Dienstleister verkauft keine standardisierte Lösung, sondern analysiert gezielt die individuellen Schwachstellen eines Unternehmens. Er sollte verständlich und ohne Fachchinesisch erklären, welche Maßnahmen notwendig sind, um die IT-Sicherheit effektiv zu verbessern und zudem einen Rund-um-die-Uhr-Support, um im Notfall sofort reagieren zu können. Achten Sie darauf, dass ein vollständiges Sicherheitskonzept entwickelt wird!

Dazu gehören eine umfassende Schwachstellenanalyse, gezielte Mitarbeiterschulungen, ein durchdachter Incident-Response-Plan sowie zuverlässige Backup- und Recovery-Strategien. Nicht zuletzt sind klare Vertragsstrukturen und ein partnerschaftlicher Ansatz, der auf langfristige Zusammenarbeit setzt, entscheidend für eine vertrauensvolle Geschäftsbeziehung.

Auch von rechtlicher Seite wird dem Thema Cybersicherheit eine immer größere Beachtung geschenkt. Welche Vorgaben zur Cybersicherheit müssen Unternehmer auf dem Schirm haben?
Ja, die rechtlichen Anforderungen an Cybersicherheit werden immer strenger, und Unternehmen müssen sich aktiv damit auseinandersetzen, um Bußgelder, Haftungsrisiken und Reputationsverluste zu vermeiden. Besonders in Europa und Deutschland gibt es klare Vorschriften, die Unternehmen zur IT-Sicherheit verpflichten. Unternehmer sollten mit der DSGVO vertraut sein und auch weitere Regelungen wie die NIS2-Richtlinie und das IT-Sicherheitsgesetz 2.0 kennen. Insbesondere für die Finanzbranche interessant ist auch der Digital Operation Resilience Act, kurz: DORA, der noch 2025 in Kraft treten wird.

Was bedeuten diese Vorgaben für die Cybersicherheitsstrategie von Unternehmen?
IT-Sicherheit ist keine Option mehr, sondern Pflicht! Unternehmen sind heutzutage verpflichtet, aktiv nachzuweisen, dass sie technische und organisatorische Schutzmaßnahmen implementieren. Ein fehlendes Schutzkonzept erhöht nicht nur das Risiko von Cyberangriffen, sondern kann auch hohe Bußgelder und Haftungsklagen nach sich ziehen. IT-Sicherheit ist daher kein nachrangiges Thema mehr, sondern ein geschäftskritischer Faktor. IT-Sicherheit darf daher nicht allein der IT-Abteilung überlassen werden, denn die Geschäftsführung kann persönlich haftbar gemacht werden, wenn sie keine angemessene Cybersicherheitsstrategie etabliert. IT-Sicherheit muss also zur Chefsache werden! Cybersicherheit ist mittlerweile eine rechtliche und wirtschaftliche Notwendigkeit. Wer sich frühzeitig mit diesen Vorgaben auseinandersetzt, kann nicht nur rechtliche Risiken minimieren, sondern sich auch gegen zukünftige Cyberangriffe besser schützen. ◆ *AS*

Bilder: Rene Schmitt, Depositphotos / welcomia

EIN FACHBEITRAG VON REHAN KHAN

Cloud-Sicherheit:

Cyberbomben entschärfen und Unternehmen schützen

Stellen Sie sich vor, Sie betreten ein Hochsicherheitsgebäude. Doch irgendwo tickt eine unsichtbare Bombe – niemand weiß genau, wann sie explodiert. Die Gefahr ist real, aber unsichtbar. Genau das passiert in der digitalen Welt täglich. Unternehmen sind permanent von Cyberangriffen bedroht, die wie scharf geschaltete Cyberbomben in ihren IT-Systemen lauern. Ein unachtsamer Klick, eine unsichere Verbindung oder eine schlecht konfigurierte Cloud-Umgebung – und schon kann der Schaden immens sein. Diese Bedrohung ist kein Szenario aus einem Science-Fiction-Film, sondern bittere Realität. Im Jahr 2023 gab es weltweit über 2,8 Milliarden registrierte Malware-Angriffe, und die Angriffe werden immer raffinierter. Mittlerweile stehen alle Unternehmen, egal ob groß oder klein, unabhängig der Branche, im Visier von Cyberkriminellen. Doch was kann man tun, wenn die Gefahr nicht greifbar ist? Genau hier setzt IT-Sicherheit an.

Warum IT-Sicherheit heute unverzichtbar ist

Die Cloud und hybrides Arbeiten haben sich als unverzichtbares Szenario für Unternehmen etabliert. Sie bieten Flexibilität, Skalierbarkeit und Effizienz – doch ohne ausreichende Sicherheitsmaßnahmen gleichen sie einem offenen Tresor. Cyberkriminelle wissen genau, dass viele Unternehmen ihre Infrastrukturen nur unzureichend absichern und nutzen diese Schwachstellen gezielt aus.

Die größten Risiken für Nutzer sind:

- Datenlecks: Unzureichend gesicherte Cloud-Daten können in falsche Hände geraten und großen Schaden anrichten.
- Ransomware: Angreifer verschlüsseln Daten und fordern ein Lösegeld – oft ohne Garantie, dass die Daten jemals wieder freigegeben werden.
- DDoS-Angriffe: Durch massenhafte Anfragen wird der Server überlastet und das Unternehmen lahmgelegt.
- Fehlkonfigurationen: Unsichere Einstellungen in Cloud-Diensten öffnen Tür und Tor für Hacker.
- Faktor Mensch: Der unsicherste Faktor in dem gesamten Zyklus ist immer noch der Mensch selbst.

Die gute Nachricht: Unternehmen können sich schützen, indem sie gezielte Maßnahmen ergreifen und eine ganzheitliche Sicherheitsstrategie implementieren.

Warum IT-Sicherheit? Die richtige Strategie für maximale Sicherheit

Die Schutzziele: Verfügbarkeit – Vertraulichkeit – Integrität! IT-Sicherheit muss in der Unternehmensstrategie verankert werden. Es reicht nicht mehr aus, dass sich nur noch die IT-Abteilung darum kümmert! IT-Sicherheit ist Chefsache! Um Cyberangriffe zu verhindern, reicht auch eine einfache Firewall längst nicht mehr aus. Effektive IT-Sicherheit besteht aus mehreren Schutzebenen – ähnlich wie das Entschärfen einer Bombe, bei dem jeder Draht sorgfältig getrennt werden muss.

»IT-Sicherheit muss in der Unternehmensstrategie verankert werden. IT-Sicherheit ist Chefsache!«
– Rehan Khan

1. Zero-Trust-Ansatz: Vertraue niemandem, überprüfe alles!
Traditionell wurden interne Netzwerke als sicher angesehen. Doch moderne Cyberangriffe passieren oft innerhalb des Unternehmensnetzwerks – sei es durch Phishing, Malware oder Insider-Bedrohungen. Der Zero-Trust-Ansatz geht davon aus, dass kein Nutzer und keine Verbindung per se vertrauenswürdig ist.

Wichtige Elemente eines Zero-Trust-Ansatzes sind:

- Multi-Faktor-Authentifizierung (MFA): Jeder Login muss doppelt abgesichert werden.
- Least Privilege-Prinzip: Nutzer erhalten nur die Berechtigungen, die sie wirklich benötigen.
- Kontinuierliche Überwachung: Jeder Zugriff wird genau geprüft, um verdächtige Aktivitäten frühzeitig zu erkennen.

2. Verschlüsselung:Der digitale Tresor für Ihre Daten
Daten sollten niemals unverschlüsselt in der Cloud gespeichert oder übertragen werden. Moderne Cloud-Sicherheitslösungen setzen auf Ende-zu-Ende-Verschlüsselung, sodass selbst bei einem Datenleck niemand die Informationen lesen kann.

Dazu gehören:

- Datenverschlüsselung in Ruhe und in Bewegung: Schutz sowohl bei Speicherung als auch bei Übertragung.
- Schlüsselmanagement-Systeme (KMS): Verwaltung kryptografischer Schlüssel, um unbefugten Zugriff zu verhindern.

3. 24/7-Überwachung durch ein Team von Sicherheitsexperten:
Cyberangriffe passieren nicht nur während der Geschäftszeiten. Eine 24/7-Überwachung durch ein Expertenteam kann Angriffe in Echtzeit erkennen und abwehren.

- KI-gestützte Bedrohungserkennung: Frühzeitiges Erkennen verdächtiger Aktivitäten.
- Automatisierte Reaktionsmechanismen: Stoppt Angriffe sofort, bevor Schaden entsteht.
- Incident Response Team: Bereitstellung schneller Gegenmaßnahmen im Ernstfall.

4. Backup-Strategien: Der Notfallplan nach der Explosion
Falls ein Angriff doch erfolgreich ist, sind regelmäßige Backups in getrennten Netzwerken und an verschiedenen Orten entscheidend. Ohne ein aktuelles Backup kann ein Unternehmen nach einem Cyberangriff mit schwerwiegenden Datenverlusten kämpfen.

Empfohlene Maßnahmen:
Automatisierte tägliche Backups: Sicherstellen, dass jederzeit eine aktuelle

- Kopie der Daten existiert.
  Immutable Backups: Unveränderliche Datenkopien, die nicht durch Ransom-
- ware manipuliert werden können.
  Disaster-Recovery-Pläne: Klare Strategie zur schnellen Wiederherstellung der
- betroffenen Systeme.
  Mitarbeiterschulungen: Die menschli-
- che Firewall stärken
  Über 80 Prozent der erfolgreichen Cyberangriffe sind auf menschliche Fehler zurückzuführen. Phishing-Mails, unsichere Passwörter und unachtsames Verhalten öffnen Hackern die Tür. Deshalb ist eine regelmäßige Security Awareness Schulung essenziell.

- **Wichtige Schulungsinhalte:**
  Phishing-Tests: Simulation realer An-
- griffe, um Mitarbeiter zu sensibilisieren.
  Passwortsicherheit: Einsatz sicherer
- Passwörter und Passwort-Manager.
  Security-by-Design-Mentalität: IT-Sicherheit als fester Bestandteil der Unternehmenskultur.

Handeln, bevor es zu spät ist!

Cyberattacken sind eine reale Bedrohung – doch mit den richtigen Maßnahmen können Unternehmen sich effektiv schützen. Dazu gehören DSGVO-konforme Cloud-Lösungen mit höchsten Sicherheitsstandards, Rund-um-die-Uhr-Überwachungen durch ein Expertenteam sowie skalierbare und flexible Sicherheitslösungen für Unternehmen jeder Größe. ◆

Bilder: Rene Schmitt, Depositphotos / welcomia

10 Tipps, die vor Cyberangriffen schützen

1. Zero-Trust-Ansatz umsetzen
Kein Nutzer oder Gerät sollte automatisch als vertrauenswürdig gelten. Multi-Faktor-Authentifizierung (MFA) aktivieren! Least-Privilege-Prinzip: Nur notwendige Zugriffsrechte vergeben und Zugriffe kontinuierlich überwachen!

2. Netzwerksicherheit optimieren
Ein sicheres Netzwerk bildet die Grundlage für effektiven Schutz vor Cyberangriffen. Segmentierung des Netzwerks, um Angriffsflächen zu reduzieren – Einsatz moderner Firewall und Intrusion Detection Systeme (IDS/IPS)! Führen Sie regelmäßige Sicherheitsupdates für Router und Switches durch.

3. 24/7-Überwachung einführen
Angriffe passieren jederzeit – daher ist permanente Kontrolle essenziell. Nutzen Sie eine KI-gestützte Bedrohungserkennung, implementieren Sie automatische Abwehrmechanismen und stellen Sie Incident-Response-Teams bereit!

4. Regelmäßige Backups erstellen
Backups sind der letzte Schutz bei Ransomware-Angriffen. Führen Sie automatische, tägliche Backups lokal in der Cloud durch! Mit Immutable Backups können Sie Ihre Daten gegen Manipulation schützen. Erstellen Sie einen Disaster-Recovery-Plan!

5. Mitarbeiter schulen
Über 80 Prozent der Angriffe erfolgen durch menschliche Fehler. Phishing-Tests regelmäßig durchführen. Nutzen Sie Passwort-Manager und sichere Passwörter! Etablieren Sie Security Awareness Programme!

6. Patchmanagement
Betreiben Sie konsequentes Patchmanagement! Um Schwachstellen mit hoher Bedrohung schnell zu schließen, eignet sich eine risikobasierte Patch-Strategie. Nutzen Sie automatisierte Patchmanagement-Systeme, um Updates zentral zu steuern und vermeiden Sie Verzögerungen. Definieren Sie SLA-basierte Update Zyklen!

7. Schutz vor Ransomware und DDoS
Cyberattacken können Geschäftsprozesse lahmlegen. Next-Generation-Firewalls (NGFW) einsetzen! DDoS-Schutz implementieren! IDS/IPS Systeme einführen!

8. IT-Sicherheitsaudits durchführen
Nur regelmäßige Prüfungen decken Schwachstellen auf. Planen Sie interne und externe Sicherheits-Audits ein und führe Sie Penetrationstests durch!

9. Notfallplan entwickeln
Schnelles Handeln minimiert Schäden bei Cyberangriffen. Hier können Incident-Response-Teams Abhilfe schaffen. Führen Sie Notfallübungen und Krisensimulationen durch!

10. Sicherheit als Prozess verstehen
IT-Sicherheit ist ein kontinuierlicher Prozess. Passen Sie Sicherheitsrichtlinien regelmäßig an und begegnen Sie neuen Bedrohungen proaktiv! ◆

»Ein sicheres Netzwerk bildet die Grundlage für effektiven Schutz vor Cyberangriffen.«
– Rehan Khan

Bilder: Rene Schmitt, Depositphotos / AndrewLozovyi

RABB
IT SOLUTIONS

Maximale IT-Sicherheit

mit unserem Cert+ Sicherheitsaudit!

Wie sicher ist Ihre IT wirklich?
Unser IT-Sicherheitsaudit nach Cert⁺ gibt Ihnen Klarheit!

Was Sie erwartet: Umfassende Analyse Ihrer IT-Landschaft – von Hardware über Software bis zur Netzwerktopologie. Detaillierter Bericht mit Schwachstellen, Risiken und Optimierungspotenzial. Vergleich mit aktuellen BSI-Grundschutz-Anforderungen, um Ihr IT-Sicherheitsniveau zu bewerten. Klarer Maßnahmenplan, um gezielt Sicherheitslücken zu schließen und Ihre IT auf das nächste Level zu heben.

Lassen Sie Ihre IT-Sicherheit professionell prüfen!

Jetzt Termin vereinbaren für eine individuelle Beratung!

Jetzt handeln!

– Schützen Sie Ihr Unternehmen vor Cyberangriffen

Cyberbedrohungen werden immer raffinierter – sind Ihre IT-Systeme optimal geschützt? Lassen Sie es nicht auf einen Angriff ankommen!

Nutzen Sie unser kostenloses Erstgespräch! In einer unverbindlichen Online-Analyse prüfen unsere IT-Sicherheitsexperten Ihren aktuellen Schutzstatus und zeigen individuelle Optimierungsmöglichkeiten auf.

Jetzt Termin sichern und Cyberrisiken minimieren!

Ihr Mehrwert:

- Identifikation potenzieller Sicherheitslücken
- Maßgeschneiderte Empfehlungen für Ihre IT-Sicherheit
- Expertenwissen ohne Verpflichtung

» Effizienz ist der Schlüssel zu erfolgreichen Managed Services. Wenn wir die richtigen Werkzeuge einsetzen und proaktiv handeln, können wir die IT-Landschaft unserer Kunden nachhaltig verbessern. «
– Rehan Khan

UNSERE VISION

Gemeinsam, sicher, zukunftsstark.

Die GSZ Cloud für alle Ihre Bedürfnisse

Willkommen bei Ihrem vertrauenswürdigen Partner für erstklassiges Hosting in Deutschland. Mit einem starken Fokus auf Sicherheit erfüllen unsere Cloud-Lösungen sämtliche Sicherheitsregularien, um Ihre sensiblen Daten optimal zu schützen.

IT Security Lösungen für den Mittelstand schnell – professionell – sicher.

Vertrauen Sie auf unsere Expertise als Sachverständige für IT-Security. Wir betrachten Ihre IT ganzheitlich im Bereich Sicherheit. Unser Angebot umfasst Audits, die Schwachstellen aufdecken und eine solide Grundlage für Sicherheitsmaßnahmen bieten. Mit unserem 24/7 Managed Service überwachen wir proaktiv Ihre Systeme, um Bedrohungen frühzeitig zu erkennen und abzuwehren.

Erstrückmeldung innerhalb von 30 Minuten – das ist unser Serviceversprechen.

Wir verstehen uns als Dienstleister, bei dem unsere Kunden im Vordergrund stehen. Daher gehört zu unserem Service nicht nur eine Erstreaktionszeit von 30 Minuten, sondern auch persönliche Ansprechpartner im Helpdesk, eine 24/7 Geräteüberwachung und regelmäßige Quartalsmeetings. Unsere Monitoringtools garantieren die Sicherheitsüberwachung ihrer Systeme und im Ernstfall können wir so schnell eingreifen und handeln. Unser Ziel ist die sichere Aufrechterhaltung und Weiterentwicklung der Infrastrukturen. Damit Sie nicht nur heute sondern auch morgen reibungslos arbeiten können.

Unsere Zertifikate

TOP 100 top100.de Top-Innovator 2024

Arbeitgeber der Zukunft digital, innovativ, modern Rabb IT Solutions GmbH Deutsches Innovationsinstitut für Nachhaltigkeit und Digitalisierung UNTERNEHMER

EUBusiness news German CEO Excellence Awards 2025 Rabb IT Solutions GmbH IT Services CEO of the Year 2025 & Innovator in Secure Cloud & Managed Services 2025

Zertifizierter Sachverständiger Gutachter DGuSV GEPRÜFT 2024 Bestätigungs-Register Nr. DE-8#17024/70-03 DGuSV Certification

WAS RABB-IT AUSMACHT

Flexibel, zuverlässig, serviceorientiert und auf Augenhöhe mit mehr als 20 Jahren Erfahrung in der IT.

Bilder: RABB IT Solutions

ERFOLG wird bei uns großgeschrieben. **Umwelt** aber auch: Das **ePaper**

Auch als ePaper-Abo.
Jetzt downloaden und lesen, was erfolgreich macht.

Besuche uns auf **www.erfolg-magazin.de/shop**
oder scanne den Code.