ES KOMMT AUF DIE RICHTIGE ABWEHR AN. SOWOHL BEI DEN RECKEN ALS AUCH IM UNTERNEHMEN. CYBER SECURITY PACKAGE

GRTNR.IT
MSSP FOR YOUR BUSINESS

WWW.GRTNR.IT | INFO@GRTNR.IT | +49 511 93689 100 | POTSDAMER STR. 12, 30916 ISERNHAGEN

CYBER-SICHERHEIT IN IHREM UNTERNEHMEN

ACHIM GÄRTNER

BODO GÄRTNER

Kölner Stadt-Anzeiger
Hackerangriff erschüttert die Republik
Hackerangriffe stehen auf der Tagesordnung
Im Brennpunkt
Kriminelle üben bei Kleinfirmen
Hacker greifen immer öfter Steuerberater und Anwaltskanzleien an – Ziel sind Daten der Mandanten
Hackerangriffe auf Kliniken
"Nur eine Frage der Zeit"
Stand: 29.01.2024 10:11 Uhr
Krankenhäuser und Pflegeeinrichtungen werden immer häufiger zum Ziel von Cyberattacken. Ein großflächiger Angriff mit vielen Ausfällen ist ein denkbares Szenario. Viele Einrichtungen sind schlecht vorbereitet.
DIGITALES
Attacke aus dem Netz
Das Böse ist oft nur einen Klick entfernt
Auch im Münsterland werden Unternehmen tagtäglich attackiert
Cyberangriffe auf Rekordhoch
Mittelstand Nachrichten
Die unterschätze Gefahr: Cyberattacken auf KMUs
Über 99 Prozent aller Unternehmen in Deutschland gehören zum Mittelstand. Dabei stellen KMUs häufig ein attraktiveres Ziel für Cyberattacken dar, als ihnen bewusst ist. Um langfristig erfolgreich zu sein, müssen sich auch kleinere und mittlere Unternehmen gegen Cyberangriffe absichern. Wie das auch ohne hohes IT-Budget oder -Ressourcen gelingt, erfahren Sie in diesem Beitrag.
Blick
Cyberattacke am Genfersee
Webseite von Schifffahrtsgesellschaft von Hackern attackiert
Cyber-Attacke auf Uni, Täter fordern Lösegeld in Bitcoin
watson
Schon wieder ein grosser Cyberangriff in der Schweiz – Hacker erbeuten 30'000 Passwörter
Suisse Velo, Anbieterin der «Suisse Velo Vignette» und weiterer Dienstleistungen rund ums Velo, ist das neuste Hacking-Opfer in der Schweiz.
Nau.ch
Pflegeheim im Hackern attackiert
Ein Alters- und Pflegeheim in Vessy im Kanton Genf ist Opfer eines Hacker-Angriffs geworden.
„Cyberattacken sind die größere Gefahr“
Russland und die USA sprechen offen über ein atomares Wettrüsten. Was bedeutet das für uns? Und wovor muss sich Österreich schützen?
Im Würgegriff der Cyberkriminellen
Vermehrte Attacken mit Schadsoftware: Warum es Angreifer auf Industriebetriebe aus Oberösterreich abgesehen haben, wie die Täter vorgehen und was der beste Schutz ist

DAS SIND WIR

Ihr Partner für Cyber-Sicherheit

- Über 40 Jahre Erfahrung in der IT
- Fokus auf Cyber-Sicherheit seit 1999
- Betreuung von KMU, Enterprise und öffentlichen Auftraggebern
- Spezialisierung auf E-Mail-Sicherheit und moderne IT-Schutzkonzepte

Unser Ansatz

- Verständliche Lösungen ohne Fachchinesisch
- Ganzheitliche Sicherheitskonzepte
- Proaktive Betreuung statt reiner Reaktion
- Technologien auf dem neuesten Stand

WARUM KMUs GLAUBEN, CYBERKRIMINALITÄT BETRIFFT SIE NICHT

- “Unser Betrieb ist doch viel zu klein für einen Angriff”
- Ransomware-Bedrohung unterschätzen
- IT-Sicherheit als Technologieproblem sehen
- Cyberhygiene missachten
- Cybersecurity keine Priorität einräumen
- Budget und Profil auseinanderklaffen lassen

E-MAIL-SECURITY: E-MAIL ALS EINFALLSTOR NR. 1

- **Über 90 % aller Angriffe starten per E-Mail**
- **Phishing-Mails sind kaum noch erkennbar**
- **Ein falscher Klick genügt**

Die Folgen
- Zugriff auf Ihr Unternehmen (& Ihre Daten!)
- Manipulierte Rechnungen
- Datenverlust oder Stillstand

Unsere Lösung
- Gefährliche E-Mails werden erkannt
- Angriffe werden blockiert, bevor sie ankommen
- Sichere Kommunikation für Ihr Unternehmen

E-RECHNUNG: NEUE PFLICHT, NEUE RISIKEN

- **E-Rechnung wird Pflicht für Unternehmen**
- **Rechnungen kommen digital und automatisiert**
- **Vertrauen in E-Mails steigt**

Das Problem
- Gefälschte Rechnungen wirken absolut echt
- Zahlungsdaten werden manipuliert
- Fehler fallen oft erst nach der Überweisung auf

Unsere Lösung
- Prüfung eingehender E-Mails und Rechnungen
- Erkennung gefälschter Absender
- Blockierung von Angriffen vor dem Posteingang

FAZIT

- Die Frage ist nicht, ob Sie es sich leisten können, in Cybersicherheit zu investieren, sondern ob Sie es sich leisten können, **es nicht zu tun**.
- Ein Angriff kann **in Sekunden** erfolgen, aber der Wiederaufbau kann Jahre dauern.
- Machen Sie Cybersicherheit zu einem **Eckpfeiler Ihrer Unternehmensstrategie** und nicht nur zu einer Fußnote in Ihrem Risikomanagement.
- Sie investieren in Gesundheitsvorsorge, machen regelmäßig Ihr TÜV beim Auto, vergessen Sie nicht die Sicherheit Ihres Unternehmens – legen Sie Ihre Unternehmenssicherheit in professionelle Hände: MSSP

CYBERANGRIFFE – ES HAFTET DIE GESCHÄFTSLEITUNG

Lassen Sie uns miteinander sprechen –

der erste Termin geht auf uns!