




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



 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

Wer bekommt die Golden Globes?
An diesem Sonntag werden im Kalifornien die Preise für Film und Fernsehen verliehen Kultur Seite 22

Kölnbarometer
Ärger über Schulen und Verkehr Seite 26, 27

KÖLN
Trotz Misserfolg
Pörsen Klick weit
Vorwärts zurück
Nach dem Tod einer Verstorbenen
an der Universität Köln werden die
Karte der Universität Köln, die
Karte der Universität Köln, die
Karte der Universität Köln, die

Hackerangriffe stehen auf der Tagesordnung

Wir leben in der globalen Ära der digitalen Erpressung. Cyberkriminelle starten täglich Tausende Erpressungsangriffe auf Unternehmen. Auch österreichische Firmen sind im Visier.



Im Brennpunkt
Vor wenigen Tagen musste die schwedische Supermarktkette Coop 800 Filialen schließen, nachdem eine Cyberattacke die amerikanische IT-Firma Kaseya lahmgelegt hatte. Wie berichtet, haben die Supermarktketten nicht mehr funktioniert, ein normaler Geschäftsbetrieb war vorübergehend nicht möglich.
Cyber-Russland - wie von Präsident Biden gesteuert - hinter den Attacken steckt, bleibt dahingestellt. Fest steht, dass das Hackerprogramm "WannaCrypt" vor vier Jahren die globale An-

sich eine Gruppierung namens DarkSide in das Netzwerk von Colonial, was massive Auswirkungen auf eine der größten Benzinpumpen der USA hatte.
Was alle Hackerangriffe gemeinsam haben? Die Cyberkriminellen fordern immer Lösegeld.
"Von der schwedischen Supermarktkette wollten die Erpresser 70 Millionen Euro kassieren, als es im März vor vier Jahren die chinesische Hackergruppe Haf-

Kriminelle üben bei Kleinfirmen

Hacker greifen immer öfter Steuerberater und Anwaltskanzleien an - Ziel sind Daten der Mandanten

zwei Jahren waren das erst 31 Prozent. Wie bei größeren Unternehmen gehe es dort um Datenklau, das Blockieren von Firmen-IT per Schadprogramm und Lösegeld, erklärt HDI-Cyberexperte Sören Brokamp. Dass zunehmend kleinere Firmen angegriffen werden, hat gleich mehrere Gründe. Zum einen sei der Schutz dort oft nicht so ausgeprägt wie bei größeren Firmen. Und: "Kleinstunternehmen fungieren unserer Erfahrung nach auch als Lernfeld, dort trainieren Cyberkriminelle für größere Unternehmen", erklärt Brokamp. Oft seien Kleinstunternehmenskanzleien das Ziel der Angriffe. Dort hätten es die Krim-

nellen auf Daten der Mandanten abgesehen, die dann erpresst würden.
"Kleinstunternehmen sind zudem Teil einer Lieferkette", sagt Brokamp. Über diese Zulieferer können Angreifer bisweilen auch in die IT-Systeme größerer Auftraggeber eindringen. Dennoch ist der materielle Schaden auch bei den Kleinfirmen spürbar. Über alle in der Studie untersuchten Firmengrößen mit bis zu 250 Beschäftigten hat HDI einen Durchschnittsschaden inklusive Lösegeld von knapp 100.000 Euro ermittelt.
Doch es lohnt sich, aktiv gegen Angriffe vorzugehen. "Ohne oder bei geringer Umsetzung von Präventionsmaßnahmen liegt ein Durchschnittsschaden wegen Betriebsunterbrechung bei 75.000 Euro, bei hoher Prävention nur bei 30.000 Euro", erklärt Brokamp. Dabei versteht er unter Prävention lediglich das kleine A-b-c des Cyberschutzes wie Antivirenprogramme, Firewall, sichere Passwörter und regelmäßige Sicherheitsupdates.
Ein Dienstleister, mit dem HDI zusammenarbeitet, hat herausgefunden, dass 60 Prozent aller Basischutz vermissen lassen. Die Wahrscheinlichkeit, dass bei einem Cyberangriff überhaupt ein Schaden eintritt, wird laut Studie allein durch die



men liegt ein Durchschnittsschaden wegen Betriebsunterbrechung bei 75.000 Euro, bei hoher Prävention nur bei 30.000 Euro", erklärt Brokamp. Dabei versteht er unter Prävention lediglich das kleine A-b-c des Cyberschutzes wie Antivirenprogramme, Firewall, sichere Passwörter und regelmäßige Sicherheitsupdates.
Ein Dienstleister, mit dem HDI zusammenarbeitet, hat herausgefunden, dass 60 Prozent aller Basischutz vermissen lassen. Die Wahrscheinlichkeit, dass bei einem Cyberangriff überhaupt ein Schaden eintritt, wird laut Studie allein durch die

Hackerangriff erschüttert die Republik

Kontakte, Chats und Adressen von Politikern und Prominenten sind im Internet verstreut. Das Cyber-Abwehrzentrum ist mit dem Fall befasst - Verdächtig ist die rechte Seite

Derzeit verheerend ein unangelegter Twitter Account namens "DIA" täglich Links zu privaten Dokumenten, die die Privatsphäre von Politikern und Prominenten gefährden. Die Cyber-Abwehrzentrale des Bundes ist mit dem Fall befasst. Die rechte Seite ist verdächtig.

Es ist ein Super-GAU für die deutsche Politik. Die Cyber-Abwehrzentrale des Bundes ist mit dem Fall befasst. Die rechte Seite ist verdächtig.

Quantität und Qualität dramatisch zusammen, sagt Prof. Sebastian Schinzel, IT-Sicherheitsexperte der Fachhochschule Münster.

Auch im Münsterland werden Unternehmen tagtäglich attackiert

Cyberangriffe auf Rekordhoch

Die unterschätzte Gefahr: Cyberattacken auf KMUs

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.

Attake aus dem Netz

Wie sich Bremer Behörden vor Cyberangriffen schützen und wie das Homeoffice Daten



Die Handelskammer hat es in der Vergangenheit geschafft, die Cyberangriffe zu verhindern. Wie werden aber die Angriffe abgewehrt? Die Bremer Behörden sind gut vorbereitet.

Das Böse ist oft nur einen Klick entfernt

immer mehr Firmen werden im Internet attackiert: Bildungswerk lädt daher LKA-Experten nach Lönningen ein



Der Kampf gegen Cyberkriminalität ist ein Dauerkampf. Die LKA-Experten werden nach Lönningen eingeladen, um die Mitarbeiter des Bildungswerks zu schulen.

Cyber-Attacke auf Uni, Täter fordern Lösegeld in Bitcoin

Die Universität Lichtenstein wurde in der Nacht von Sonntag auf Montag Opfer einer Cyber-Attacke. Die Täter fordern Lösegeld in Bitcoin.

Webseite von Schiffahrtsgesellschaft von Hackern attackiert

Hacker haben Ende August die Internetseite der Schiffahrtsgesellschaft CGN angegriffen. Bei Ticketkaufsystem gelang es den Tätern, die

Pflegeheim im Hackern attackiert

Ein Alters- und Pflegeheim in Vessy im Kanton Genf ist Opfer eines Hacker-Angriffs geworden. Die Heimleitung erstattete Anzeige gegen Unbekannt. Sie kann nicht ausschließen, dass die gestohlenen Daten der Bewohnerinnen und Bewohner im Darknet im Internet auftauchen.

Schon wieder ein grosser Cyberangriff in der Schweiz - Hacker erbeuten 30'000 Passwörter

Suisse Velo, Anbieterin der «Suisse Velo Vignette» und weiteren Dienstleistungen rund ums Velo, ist das neuste Hacking-Opfer in der Schweiz. Die Täter erbeuteten rund 30'000 E-Mail-Adressen und Passwörter.

„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



Die unterschätzte 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.

Wenn es bereits zu spät ist, fragt man sich: Wie konnte das nur passieren? Die größten Bedrohungsszenarien für ein Unternehmen entstehen in der heutigen Zeit nicht innerhalb der Fertigungsindustrie oder im Großraumlager, sondern in der IT-Infrastruktur des Unternehmensnetzwerk. Hier legen immer öfter Verschlüsselungsprobleme und gezielte Angriffe aus aller Welt den gesamten Betrieb lahm. Eine Studie von Bitkom wurden letztes Jahr neun von zehn Unternehmen von einer Cyberattacke. Auch der Schaden auf die Unternehmen ist in den letzten zwei Jahre auf 234 Millionen Euro gestiegen.

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!

