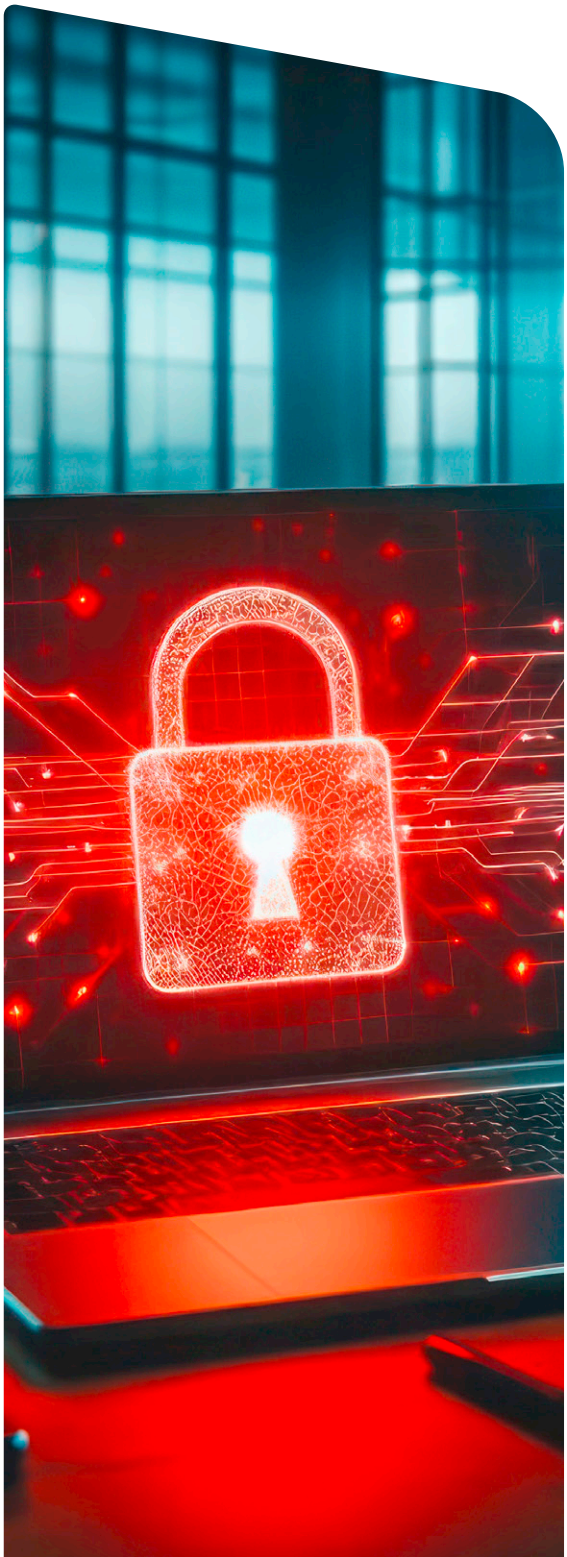
MediaMarktSaturn Business

Cyberattacken nehmen zu: So schützen Sie Ihr Business effektiv

Cyberangriffe nehmen stetig zu. Der wirtschaftliche Schaden durch Phishing, Ransomware und Co. liegt dabei regelmäßig über 200 Milliarden Euro pro Jahr. Zunehmend geraten auch kleine und mittlere Unternehmen ins Visier der Hacker. Es wird Zeit, wirksame Gegenmaßnahmen zu ergreifen.

KMU immer häufiger betroffen

72 Prozent der deutschen Unternehmen wurden 2022/2023 Opfer einer Attacke auf ihre Daten. Weitere 8 Prozent vermuten, dass sie angegriffen wurden – denn mancher Angriff hinterlässt kaum Spuren. Das zeigt die aktuelle Wirtschaftsschutz-Studie des Digitalverbands Bitkom (September 2023). Durch Datendiebstahl, Industriespionage und Sabotage entstanden der deutschen Wirtschaft demzufolge Schäden von mehr als 200 Milliarden Euro.



Dabei verlagern sich die Attacken immer weiter in den digitalen Raum. Phishing, Passwortdiebstahl und Schadsoftware stehen laut der Befragung von über 1.000 Unternehmen ganz oben auf der Liste der digitalen Angriffe. Wenig verwunderlich also, dass mehr als jeder zweite deutsche Betrieb in Cyberattacken eine große Bedrohung sieht.

Stellen Sie sich vor, Sie kommen morgens ins Büro und stellen einen Cyberangriff fest. Nichts geht mehr. All Ihre Kundendaten sind verschwunden – gestohlen von Hackern, die Ihre Schwachstellen ausgenutzt haben. Es drohen Lösegeldforderungen, Schadenersatz und Strafzahlungen, falls geltende Regelungen zur Cybersicherheit verletzt wurden. Von irreparablen Rufschäden ganz zu schweigen.

Leider ist das kein unrealistisches Szenario – gerade für kleine und mittlere Unternehmen (KMU). Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) geraten diese zunehmend ins Visier von Cyberkriminellen. Denn sie arbeiten mit wertvollen Datenbeständen, verfügen jedoch oft nur über begrenzte Budgets für die Cybersicherheit. Laut BSI greifen Hacker dabei vielfach nicht zielgerichtet an. KMU werden stattdessen häufig von automatisierten, großflächigen Angriffen getroffen.

Diese Attacken sind häufig erfolgreich, wenn simple Grundregeln nicht beachtet werden und die Belegschaft für die Gefahren nicht sensibilisiert ist.

Individuelle Beratung durch Experten erforderlich

KMU – wie beispielsweise Handwerksbetriebe oder Einzelhändler – die keine Spezialisten für Informationstechnik und Cybersicherheit beschäftigen, sollten auf die Beratung durch externe Experten setzen, empfiehlt das BSI. Diese beraten umfassend und individuell zu IT-Ausstattung und -Sicherheit.

Auch Fachhändler für IT-Hardware wie MediaMarktSaturn als Europas größter Fachhändler für IT-Hardware bietet mit seiner Business-Sparte eine Vielzahl von Dienstleistungen und individuellen Lösungen, um die IT-Infrastruktur und Cybersicherheit kleiner und mittlerer Unternehmen zu optimieren.

Das BSI empfiehlt, dass KMU „proaktive Schritte unternehmen, um ihre Netzwerke und Daten zu schützen“. Dazu gehörten regelmäßige Schulungen der Angestellten, die Aktualisierung von Systemen und Software sowie das Implementieren von Best Practices in der Cybersicherheit. Mit individuellen technischen Lösungen, aber auch mit klaren Verhaltensregeln für die Belegschaft und erhöhter Sensibilität für die Gefahren errichten Unternehmen einen wirkungsvollen digitalen Schutzschild gegen die sich verschärfende Bedrohungslage. Die gute Nachricht: Es gibt ein ganzes Bündel an Basismaßnahmen, die KMU schnell ergreifen können.

Effektive Basismaßnahmen für die IT-Sicherheit Ihres Unternehmens:

Sensibilisieren Sie Ihre Mitarbeiter:

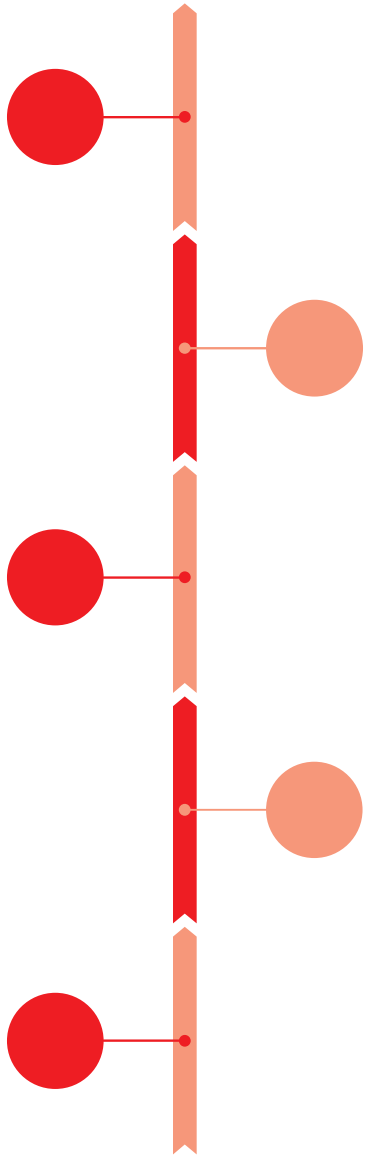
Phishing-Seiten oder -Mails werden immer schwerer erkennbar. Halten Sie Ihre Angestellten mit regelmäßigen Workshops auf dem neusten Stand.

Regelmäßige Updates:

Sorgen Sie dafür, dass alle verwendeten Programme stets auf dem neusten Stand sind. Sicherheits-Patches und Updates sollten stets zeitnah installiert werden, um vorhandene Sicherheitslücken umgehend zu schließen.

IT-Beratung und Support:

Lassen Sie sich von erfahrenen Beratern dabei unterstützen, Ihre IT-Infrastruktur zu optimieren und individuelle Lösungen zu implementieren.



Multi-Faktor-Authentifizierung:

Dieses Verfahren schafft Sicherheit über eine Bestätigung eines Logins auf einem externen Gerät (Smartphone) oder per Mail.

Backup und Desaster Recovery:

Ein effektiver Backup-Plan ist entscheidend, um Ihre Daten im Falle eines Cyberangriffs oder Systemausfalls zu schützen und im Notfall schnell wiederherzustellen.

Weiterführende empfehlenswerte Maßnahmen sind beispielsweise

Einführung eines Mobile Device Management Systems (MDM), mit dem Sie die Berechtigungen der Nutzer auf jedem Gerät beschränken und diese aus der Ferne warten und sperren können.

Überwachung und Protokollierung des Datenverkehrs im Firmennetzwerk, um verdächtige Aktivitäten zu erkennen.

Netzwerksegmentierung, um die Infiltration Ihrer Systeme zu erschweren.

Wenig überraschend: 82 Prozent der in der Wirtschaftsschutz-Studie befragten Unternehmen rechnen mit einer weiteren Zunahme von Cyberangriffen. Der Appell muss also lauten: Investieren Sie in Cybersicherheit – für die Zukunft Ihres Unternehmens.

Finden Sie passende Lösungen und Ihren persönlichen Ansprechpartner:

mediamarkt.de/de/b2b-registration;
saturn.de/de/b2b-registration

Ansprechpartner

Stefan Köstler
Head of National Sales

Per Mail:
geschaeftskunden.vertrieb@mediamarkt.de
vertrieb.business@saturn.de

Sie suchen IT-Lösungen aus einer Hand? Als Europas größter Fachhändler für Elektronikprodukte unterstützen wir Ihr Business mit einem persönlichen Ansprechpartner, einem riesigen Sortiment und unabhängiger Beratung. Ganz egal, ob Solo-Selbstständig, KMU oder Großunternehmen, ob Start-Up, öffentliche Verwaltung oder Gastrobetrieb: Als Geschäftskunde von MediaMarktSaturn machen Sie mehr aus Ihrem Business.

MediaMarktSaturn Business

MediaMarkt SATURN