Pressemitteilung

06.10.2020

IT-Systemausfall! Und dann?

>> Viele Unternehmer schenken dem Schutz vor möglichen IT-Ausfällen zu wenig Beachtung. Was muss im Notfall beachtet werden und welche Rolle spielen die Mitarbeiter dabei?

>>>Mit Unified Security Cert+ gibt es einen neuen IT-Sicherheitsstandard für kleine und mittlere Unternehmen

Tagtäglich hören wir in den Medien von Hacker-Angriffen auf private und geschäftliche Computer und Netzwerke. Die Gefahr für Unternehmen, Opfer eines Cyberangriffs zu werden, ist so groß wie nie zuvor. Doch wie verhält man sich, wenn man tatsächlich Opfer eines solchen Angriffs geworden ist? Und welche Rolle spielen eigentlich die Mitarbeiter beim Thema IT-Sicherheit?

Über 70 % der IT-Sicherheitsvorfälle werden durch den Menschen ausgelöst. Teils vorsätzlich, meistens jedoch durch Unkenntnis oder Fahrlässigkeit. Hier einige Beispiele: Der „vergessene“ USB-Stick liegt z. B. auf dem Mitarbeiter-Parkplatz. Und da der Mensch von Natur aus neugierig ist, nehmen wir ihn natürlich mit und stecken ihn in den nächsten Rechner. Phishing-Mails von Banken, Krankenkassen, Behörden oder Bewerbern sind leider nicht mehr auf den ersten Blick zu erkennen und von „echten“ Absendern kaum zu unterscheiden. Täuschend echte Nachrichten von Freunden und Kollegen haben in der Cyberkriminalität eine hohe Erfolgsquote. Denn in einer Mail von einem bekannten Absender wird keine Gefahr bzw. kein Risiko vermutet. Die Opfer werden von Social Engineers gerne in sozialen Netzwerken ausspioniert.

„Um die Sicherheit ihrer IT zu gewährleisten, sollten Unternehmen ihre Mitarbeiter regelmäßig schulen und für die Gefahren sensibilisieren“, weiß Markus Krieg vom IT-Dienstleister BREKOM aus Paderborn. „Und dies sollte im besten Fall so erfolgen, dass Arbeitnehmer sich betroffen fühlen. Durch die Betroffenheit wird mehr IT-Bewusstsein geschaffen.“ Dazu eignen sich Online-Schulungen mit praxisrelevanten Trainingsinhalten, die interaktiv und verständlich vermittelt werden.

Viele Unternehmen wissen, dass von einer funktionierenden IT langfristig der Erfolg und das Vertrauen der Kunden abhängt. Einige Mittelständler hoffen, dass ein Cyberangriff oder Systemausfall im eigenen Unternehmen nicht vorkommt, andere verlassen sich ausschließlich auf die IT-Verantwortlichen. Eine verantwortungsbewusste Geschäftsleitung muss sich daher die Frage stellen, welche konkreten Schutzmaßnahmen für die eigene IT-Infrastruktur getroffen werden müssen. Während große Unternehmen dafür eine eigene Abteilung und Fachleute im Haus haben, suchen kleine und mittlere Unternehmen (KMU)

Dies ist eine Pressemitteilung der BREKOM GmbH.
Pressekontakt BREKOM:

Silke Heitmann, Tel. 0421 2400 1200, E-Mail: presse@brekom.de
BREKOM GmbH, Am Weser-Terminal 1, 28217 Bremen

nach bezahlbaren Lösungen und anwendbaren Maßnahmen. Oft fehlt es jedoch an Orientierung, was genau KMU im Bereich IT-Sicherheit benötigen und welche Schritte dafür notwendig sind. Einzelne Tipps helfen kaum, eine gute Schutzstrategie zu entwickeln. Gleichzeitig sind Konzepte wie „BSI-Grundschutz“ und der ISO 27001-Standard für KMU zu komplex, zu aufwendig und schlicht zu teuer.

„Häufig scheitert es schon an den hohen Einstiegshürden“, hat Markus Krieg von BREKOM beobachtet. „Unified Security Cert+ schließt diese Lücke und macht es einfacher.“ Der neue, unabhängige Standard fokussiert sich im Vergleich zu anderen Standards auf Maßnahmen, die für kleine und mittlere Unternehmen in der Praxis leistbar sind. Dadurch erreichen KMU schnell ein besseres IT-Sicherheitsniveau und können die erreichten Sicherheitslevel stufenweise zertifizieren lassen. Mit diesen Zertifikaten kann das Unternehmen den Level der IT-Sicherheit und der Datenschutz-Konformität (EU DS-GVO) seinen Kunden transparent darstellen und deren Bedeutung hervorheben.

Mit einem guten Notfallplan haben Unternehmen im Falle eines Systemausfalls keine größeren Verluste zu befürchten. Es sollen möglichst wenige Daten verloren gehen und die IT sollte in möglichst kurzer Zeit wieder funktionstüchtig sein. Ein guter Plan verhindert somit Zeitverlust und finanzielle Schäden. Er sollte beispielsweise auf folgende Fragen Antworten enthalten: Was passiert, wenn die IT ausfällt? Welche Unternehmensbereiche sind bei Ausfall welcher Systeme betroffen? Welche Ausfallzeiten kann ich mir als Unternehmen leisten? Welche Maßnahmen müssen ergriffen werden, um die Systeme wieder zum Laufen zu bringen?

Ein vorbereiteter Handlungsplan ist der Rettungsanker für die IT. Ein Notfall kommt immer in einer ungünstigen Situation und ist meistens die Verkettung von einzelnen Störungen, die jeweils nicht kritisch gewesen wären. Der Wettlauf mit der Zeit beginnt. „Eine strukturierte Notfallplanung ist daher auch für mittelständische Unternehmen unverzichtbar. Sie erspart im Ernstfall deutlich mehr Arbeit und Stress, als sie im Vorfeld verursacht“, so Markus Krieg vom IT-Dienstleister BREKOM. Durch den Blick eines Externen mit einem strukturierten Fragenkatalog können ohne viel Aufwand bedarfsgerechte Maßnahmen ausgewählt werden, um die Sicherheit zu steigern und IT-Ausfällen professionell und geplant begegnen zu können.

Weitere Informationen sind im Internet zu finden unter: https://brekom.de/it-service-owl

Dies ist eine Pressemitteilung der BREKOM GmbH.
Pressekontakt BREKOM:

Silke Heitmann, Tel. 0421 2400 1200, E-Mail: presse@brekom.de
BREKOM GmbH, Am Weser-Terminal 1, 28217 Bremen

Über BREKOM

BREKOM bietet als Partner für Kommunikation und Sicherheit Geschäftskunden individuell durchdachte 360° Solutions in den Bereichen IT, Communication, Managed Services, und Safety & Security an. Als Tochterunternehmen der EWE TEL GmbH verbindet sich bei BREKOM die persönliche Nähe eines mittelständischen Unternehmens mit der Leistungsfähigkeit eines Konzerns. Mit der Expertise von über 150 Mitarbeiterinnen und Mitarbeitern aus dem Stammsitz in Bremen sowie aus der Niederlassung Ostwestfalen-Lippe (Paderborn und Bielefeld) findet BREKOM im Dialog mit dem Kunden hochwertige Lösungskonzepte, die optimal zum Kundenbusiness passen und sich auch langfristig als leistungsstark erweisen. Mit diesen Dienstleistungen aus einer Hand bleibt Geschäftskunden aus allen Branchen sowie Institutionen und Behörden mehr Freiraum, sich um ihr Kerngeschäft zu kümmern. Innovative Technologie, Erfahrung und qualitativ hochwertige Dienstleistungen sind die Säulen, auf denen BREKOM sich stetig weiterentwickelt und als Unternehmen wächst. Weitere Informationen finden sich im Internet unter www.brekom.de.

Über Markus Krieg

Markus Krieg ist seit über 20 Jahren im IT-Business tätig. Als Leiter der BREKOM Business Unit Ostwestfalen-Lippe betreut er mit seinem Team Geschäftskunden in der Region. Als IT-Experte berät, erstellt und implementiert er IT-Lösungen für Unternehmen. Der Fokus liegt darauf, den Kunden eine stabile und reibungslos funktionierende IT zur Verfügung zu stellen, damit Sie sich jederzeit auf Ihr Kerngeschäft konzentrieren können. Seine langjährigen Erfahrungen im Bereich des IT-Outsourcings und der IT-Security machen ihn zu einem Kenner der Thematik und ersten Ansprechpartner für den Mittelstand.

Dies ist eine Pressemitteilung der BREKOM GmbH.
Pressekontakt BREKOM:

Silke Heitmann, Tel. 0421 2400 1200, E-Mail: presse@brekom.de
BREKOM GmbH, Am Weser-Terminal 1, 28217 Bremen