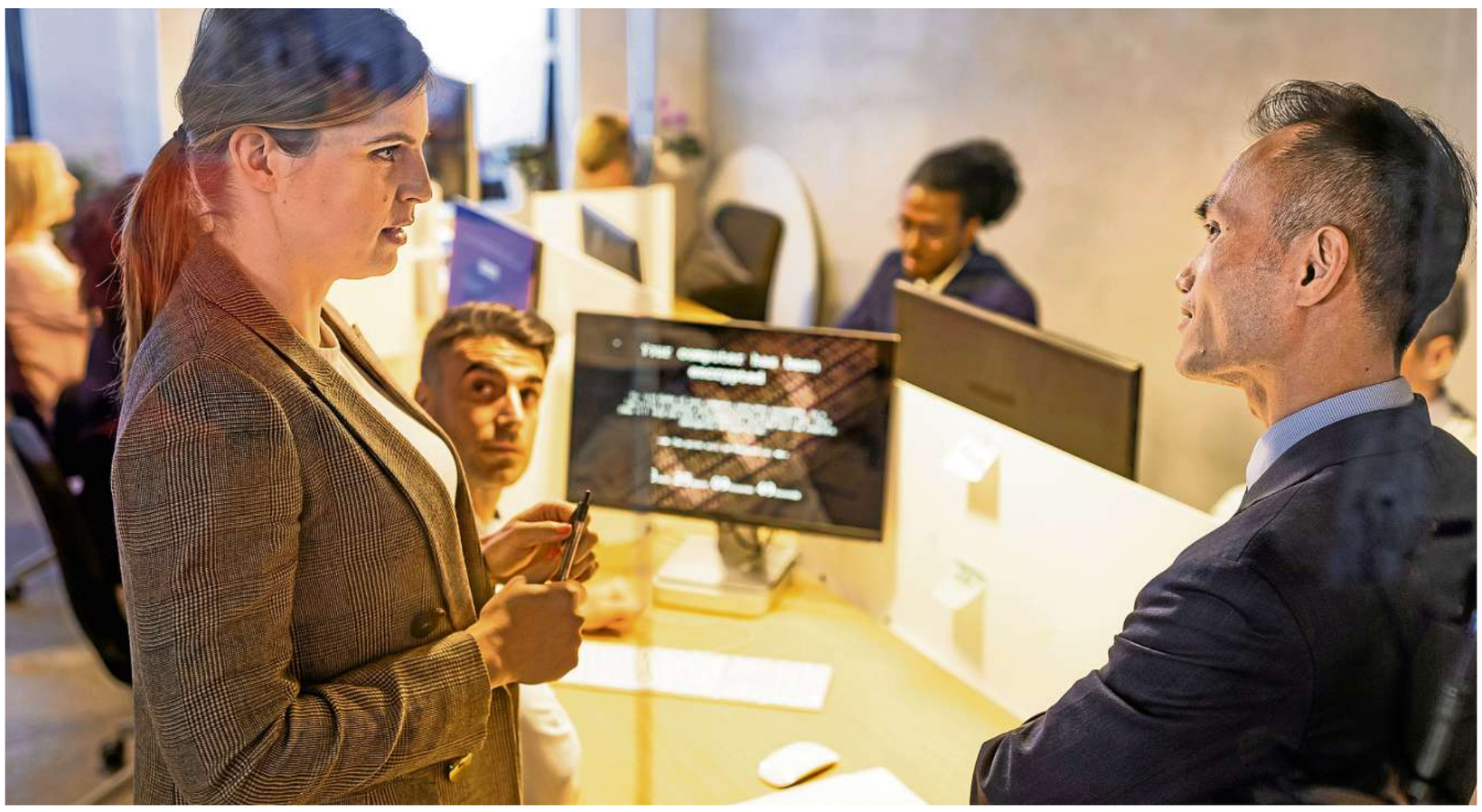
RATGEBER

Wie sich Firmen vor Cyberangriffen schützen

Die Digitalisierung bringt große Datenmengen mit sich. Sie sicher zu verwalten, stellt Unternehmen vor Herausforderungen

Chan Sidki-Lundius



Auch kleine und mittelständische Unternehmen sollten unbedingt in ihre IT-Sicherheit investieren, um ihre Daten und ihre Infrastruktur zu schützen. Sonst kann es im Falle eines Cyberangriffs sehr teuer werden. NOSYSTEM IMAGES / GETTY IMAGES

Hamburg. Nicht nur in Hamburg machen sich viele Unternehmen Sorgen, dass der russische Krieg gegen die Ukraine verstärkt auch im Cyberraum geführt wird. So gehen 73 Prozent der deutschen Startups von einer verschärften Bedrohungslage für das eigene Unternehmen aus. Das ist das Ergebnis einer Umfrage des Digitalverbands Bitkom. „Der russische Krieg gegen die Ukraine wurde von Beginn an auch im Cyberraum geführt", bestätigt Bitkom-Präsident Achim Berg.

Unternehmen, deren Geschäftserfolg auf der Nutzung von digitalen Technologien und Daten basiert, sollten sich daher besonders wirksam schützen. Zusammen mit der ohnehin seit Jahren steigenden Cyberkriminalität gelte es, so Berg, die eigenen Sicherheitsvorkehrungen zu überprüfen und wo nötig nachzubessern. Der Digitalverband Bitkom gibt konkrete Tipps, welche Vorbereitungen und Vorsichtsmaßnahmen insbesondere kleine und mittelständische Unternehmen jetzt treffen sollten

Die firmeninterne IT-Infrastruktur sollte immer auf dem aktuellen Stand sein

Unternehmen sollten ihre Schutzmaßnahmen insgesamt verstärken. Betriebssysteme und Software müssen auf dem aktuellen Stand sein, Sicherheitsupdates sind zügig einzuspielen. Sichere, also komplexe und für jedes System unterschiedliche, Passwörter tragen signifikant zur Erhöhung des Schutzniveaus bei. Außerdem sollten möglichst alle Logins mit Außenanbindung über eine Multi-Faktor-Authentifizierung geschützt werden. Für einzelne Nutzerinnen und Nutzer sollten Privilegien und Administrationsrechte eingeschränkt werden und die Komplexität von verwendeten Diensten insgesamt verringert werden.

Eine solche Härtung der Systeme ist trotz Einschränkung der Nutzungsfreundlichkeit und Produktivität zum Schutz der eigenen Infrastruktur und unternehmenssensiblen Daten unbedingt ratsam. Zudem ist die unternehmenseigene Back-up-Strategie zu prüfen und nachzuziehen, sodass alle relevanten Unternehmensdaten gesichert sind und zusätzlich Sicherheitskopien offline auf einem externen Datenträger existieren.

Unternehmen müssen in einem Angriffsfall reaktionsfähig sein. Aus diesem Grund braucht es die klare Definition von Verantwortlichkeiten im Sicherheitsbereich und die Einrichtung entsprechender Anlaufstellen – sowohl intern als auch bei externen Dienstleistern. Außerdem sollte sichergestellt sein, dass zu jeder Zeit ausreichend Personal einsatzfähig ist. Urlaubszeiten oder Vertretungen bei Krankheit sind bei dieser Planung mit einzukalkulieren.

Die Erfahrungen zeigt: Der Mensch bleibt eines der größten Sicherheitsrisiken, ist gleichzeitig aber auch Schutzgarant eines Unternehmens. Alle Beschäftigten sind daher für das erhöhte Risiko von Cyberangriffen zu sensibilisieren. Dazu gehört, potenzielle Gefahren verständlich zu erklären und Schritt-für-Schritt-Anleitungen bereitzustellen, wie man sich im Falle eines Angriffs verhält und an wen man sich wenden muss.

Gegebenenfalls können kurzfristige Sicherheitsschulungen sinnvoll sein. Ziel ist es, die Wachsamkeit in der Belegschaft zu erhöhen. Insbesondere für den E-Mail-Verkehr gilt: Hyperlinks und Anhänge sind nicht vorschnell zu öffnen und ungewöhnliche Anweisungen mit Skepsis zu betrachten.

Besonderes Augenmerk sollten die Verantwortlichen darauf legen, Mitarbeiter über sogenannte Phishing-Mails, das sind gefälschte E-Mails, aufzuklären. Sie werden immer professioneller: Eine unpersönliche Anrede, Tippfehler, seltsame Umlaute oder in schlechtem Deutsch verfasste Texte sind eher selten und für das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein eindeutiger Hinweis auf einen Phishing-Versuch.

Auch bei gut formuliertem Text und insbesondere bei folgenden Punkten sollten Unternehmen wachsam sein, so das BSI: Der Text der E-Mail gibt dringenden Handlungsbedarf vor oder es werden Drohungen ausgesprochen. Vorsicht ist auch geboten, wenn man aufgefordert wird, vertrauliche Daten (etwa eine PIN oder eine Kreditkartennummer) einzugeben oder wenn die E-Mail unbekannte Links oder Formulare enthält. Und schließlich sollten Sie misstrauisch werden, wenn Sie E-Mails von einer Ihnen bekannten Person oder Organisation erhalten und Ihnen das entsprechende Anliegen des Absenders unseriös vorkommt.

Übrigens: Die volkswirtschaftlichen Schäden von Cyberdelikten, die mit Pishing-Attacken beginnen, werden in Deutschland pro Jahr mindestens auf einen zweistelligen Millionenbetrag geschätzt.

Jedes Unternehmen sollte einen konkreten Notfallplan erstellen

Für den Fall eines Angriffs sollte im Unternehmen ein Notfallplan bereitliegen, der das weitere Vorgehen dokumentiert. Neben den technischen Schritten, die eingeleitet werden müssen, sollte der Plan auch organisatorische Punkte wie die Kontaktdaten relevanter Ansprechpersonen im Unternehmen sowie die Notfallkontakte der offiziellen Anlaufstellen beinhalten. Auch rechtliche Aspekte wie Meldepflichten bei Datenschutzverletzungen müssen berücksichtigt werden. Des Weiteren ist eine vorbereitete Krisenkommunikation empfehlenswert, um schnell alle relevanten Stakeholder wie Kunden, Partner sowie die Öffentlichkeit zu informieren.

Die Sicherheitslage ist hochdynamisch und kann sich von Tag zu Tag ändern. Unternehmen sollten daher die Meldungen der Behörden unbedingt regelmäßig verfolgen. Erste Adressen sind das Bundesamt für Sicherheit in der Informationstechnik sowie die Allianz für Cybersicherheit.

www.bsi.bund.de
www.allianz-fuer-cybersicherheit.de

Betriebe suchen verstärkt Sparpotenziale

Vor allem Wasser- und Energieversorger haben Beratungsbedarf

Hamburg. Angesichts wachsender Krisenfaktoren in der deutschen Wirtschaft treten immer mehr Unternehmen auf die Kostenbremse. Auch Programme zur Effizienzsteigerung nehmen Fahrt auf. Für die Consultingbranche bedeutet dies, dass die Nachfrage der Kunden nach klassischen Restrukturierungs- und Sanierungsthemen steigt. Dazu Ralf Strehlau, Präsident des Bundesverbands Deutscher Unternehmensberatungen (BDU): „Der Putin-Krieg, Lieferengpässe, Krisenszenarien bei der Energieversorgung und die hohe Inflationsrate lassen bei den Unternehmen zunehmend die Alarmglocken läuten. Die Konsequenz: Wirtschaft und Industrie machen sich mit Unterstützung von uns Consultants möglichst schnell und umfassend krisenfest."

Im Ranking der Kundenbranchen mit der stärksten Nachfrage nach Beratungsleistungen hat sich bei der aktuellen Geschäftsklima-Befragung des BDU die Energie- und Wasserversorgungsbranche nach vorn geschoben. Der deutsche Beratungsmarkt wird von internationalen Consultants dominiert, von denen viele auch in Hamburg vertreten sind. Marktführer sind die internationalen Strategieberatungen McKinsey, BCG und Bain, gefolgt von den Advisory-Einheiten der großen Wirtschaftsprüfungsgesellschaften Deloitte und Pricewaterhouse Coopers sowie der Consulting-Einheit von Accenture.

Dass die Akzeptanz für Remote-Projekte, das sind solche, bei denen Teammitglieder aus der Ferne zuarbeiten, infolge der Corona-Pandemie sowohl unter Consultants als auch deren Beratungskunden deutlich angestiegen ist, zeigt das aktuelle Themendossier „Remote Consulting – Managementberatungsprojekte erfolgreich umsetzen" des Marktforschungs- und Beratungsunternehmens Lünendonk & Hossenfelder.

Dennoch begrüßen rund 60 Prozent der befragten Berater und Mandanten einen persönlichen Erstkontakt. Sei der Kontakt einmal hergestellt, könnten Beratungsprozesse ohne Schwierigkeiten mit Vertrauen auch über Onlinetools abgebildet werden. Das Themendossier steht online unter www.luenendonk.de kostenfrei zum Download bereit. *csl*