Bitkom e.V. |

Wie sich die deutsche Wirtschaft gegen Diebstahl, Spionage und Sabotage schützt

- **Höheres Risikobewusstsein: Unternehmen setzen zunehmend auf Abwehrmaßnahmen**
- **59 Prozent benennen Sicherheitsverantwortliche; 22 Prozent planen den Einsatz**
- **Nur jedes zweite Unternehmen verfügt über Notfallmanagement-Plan für Angriffsfall**

Berlin, 14. Oktober 2021 - Diebstahl, Spionage und Sabotage können jedes Unternehmen treffen und zu einer existenziellen Gefahr werden. Doch nur die Hälfte der Betriebe im Land verfügt über geregelte Abläufe und Sofort-Maßnahmen, also ein Notfallmanagement, für den Ernstfall. In 51 Prozent der Firmen gibt es Regelungen, 44 Prozent der Unternehmen verfügen nicht über Notfall-Konzepte. Das ist das Ergebnis einer repräsentativen Umfrage des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen befragt wurden. Seinen Bericht zu den von der deutschen Wirtschaft getroffenen Sicherheitsmaßnahmen hat der Bitkom heute erstmals veröffentlicht.

„Jedes Unternehmen braucht geregelte Abläufe und Sofort-Maßnahmen für den Notfall. Besonders entscheidend ist ein Notfallmanagement für Unternehmen der kritischen Infrastruktur, etwa Krankenhäuser oder Energieversorger. Denn wir müssen davon ausgehen, dass das Angriffsgeschehen künftig weiter zunehmen wird“, sagt Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung.

Nur die Hälfte der Unternehmen setzt auf Zwei-Faktor-Authentifizierung

Mit seiner Studie gewährt der Bitkom einen umfangreichen Einblick in die von der deutschen Wirtschaft getroffenen Absicherungsmaßnahmen: Demnach setzen aktuell 72 Prozent der Unternehmen Mindestanforderungen an Passwörter, etwa in Form von zwingend erforderlichen Sonderzeichen oder Sperrlisten. Weitere 16 Prozent planen solche Anforderungen. 71 Prozent protokollieren, welche Mitarbeitenden auf welche Daten oder Laufwerke zugreifen (10 Prozent geplant), 70 Prozent kontrollieren den Zugang zu Gebäuden oder Maschinen elektronisch (13 Prozent geplant) und 67 Prozent verschlüsseln Daten auf Datenträgern (12 Prozent geplant).

Im Zuge der Corona-Pandemie hat besonders die Absicherung von Cloud-Anwendungen an Bedeutung gewonnen. Sie sind vielfach notwendig, um Mitarbeitenden die Arbeit aus dem Homeoffice zu ermöglichen. 63 Prozent haben hierzu Schutzmaßnahmen im Einsatz; weitere 25 Prozent haben das geplant.

Allerdings werden viele weitere Sicherheitsmaßnahmen von etlichen Unternehmen im Land nicht genutzt: 60 Prozent setzen zwar auf abhörsicherer Sprachkommunikation, nur 46 Prozent allerdings auf erweiterte Verfahren zur Benutzeridentifikation – also etwa die Anmeldung auf einem Gerät mittels Zwei-Faktor-Authentifizierung (z.B. Bestätigung per App oder SMS auf einem weiteren Gerät). Gegen den Datenabfluss von innen sichern sich 43 Prozent ab, 42 Prozent separieren Netzwerkzugänge für Kunden oder Geschäftspartner und 41 Prozent verschlüsseln ihren Mailverkehr.

„Viele Sicherheitsmaßnahmen lassen sich mittlerweile leicht umsetzen und mit wenig Vorlaufzeit im Arbeitsalltag integrieren. Trotzdem steigt deren Nutzung nur langsam. Die Zuwächse sind zwar grundsätzlich ein positives Signal, Unternehmen sollten aber keine Zeit verlieren ihre Sicherheit ausbauen“, kommentiert Bitkom-Geschäftsleiterin Dehmel.

Unternehmen definieren klare Regeln für Umgang mit sensiblen Daten

Neben technischen Sicherheitsmaßnahmen bauen Firmen vor allem auf organisatorische

Vorkehrungen, zeigt die Bitkom-Studie. Demnach setzten zuletzt sämtliche Unternehmen darauf, bestimmte Informationen mit Zugriffsrechten zu versehen. Klare Regeln für den Umgang mit schützenswerten Informationen gab es in 86 Prozent der Betriebe. Die Zutrittsrechte für bestimmte Räume waren in 83 Prozent der Firmen reguliert.

Starken Zulauf im Pandemiejahr erlebte die Clean-Desk-Policy, die festlegt, wie Mitarbeitende mit vertraulichen Informationen an ihrem Arbeitsplatz umgehen müssen. Sensible Dokumente wie Passwortzettel dürfen demnach nicht ungeschützt zugänglich oder sichtbar auf dem Schreibtisch verbleiben. Diese Regel gilt in 68 Prozent der Unternehmen, zehn Prozent planen den Einsatz. Im Jahr 2019 galten solche Maßnahmen nur bei 55 Prozent der Firmen; 2017 war das bei 51 Prozent der Fall.

Ob diese und weitere Regeln eingehalten werden, können im Betrieb etwa Sicherheitsverantwortliche überprüfen: 59 Prozent haben solche Mitarbeitenden bereits im Einsatz, 22 Prozent planen dies. Zwei Jahre zuvor lag der Wert noch bei 50 Prozent. Eine Schulung der Mitarbeitenden zu Sicherheitsthemen nehmen 56 Prozent vor. Dazu Bitkom-Expertin Dehmel: „Unvorsichtige oder schlecht geschulte Beschäftigte können schnell zum Ziel von Angriffen werden. Investitionen in Schulungen sind deshalb immer auch wichtige Investitionen in die Zukunft des Unternehmens. Dabei ist zentral, die Mitarbeitenden gezielt für ihren spezifischen Arbeitskontext weiterzubilden."

Geht es um die Besetzung sensibler Positionen, führen 55 Prozent der Firmen Background-Checks durch; überprüfen also den beruflichen und persönlichen Hintergrund von neuen Mitarbeitenden. Zudem setzen Firmen verstärkt auf Whistle-Blowing-Tools, ermöglichen es Mitarbeitenden also, anonyme Hinweise zu geben. Nach eigenen Angaben ist ein solches Instrument bei 32 Prozent der Unternehmen im Einsatz, 11 Prozent planen dies. Im Jahr 2019 nutzten nur 23 Prozent diese Möglichkeit, 2017 waren es 16 Prozent.

Die Bitkom-Umfrage zeigt zudem, inwieweit Managementsysteme für Informationssicherheit (ISMS) in der deutschen Wirtschaft im Einsatz sind und ob gültige Sicherheits-Zertifizierungen gehalten werden.

Die Ergebnisse stehen zum kostenlosen Download unter diesem Link bereit: https://www.bitkom.org/Bitkom/Publikationen/Sicherheitsmassnahmen-2021-Chart-Bericht-zur-IT-Sicherheit-in-der-deutschen-Wirtschaft.

Hinweis zur Methodik: Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.067 Unternehmen mit 10 oder mehr Mitarbeiterinnen und Mitarbeitern befragt. Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführerinnen und Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen. Die Umfrage ist repräsentativ für die Gesamtwirtschaft.

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org

Felix Kuhlenkamp
Bereichsleiter Sicherheitspolitik
Nachricht senden
