Cyberattacken wirksam begegnen - HDI Studie sieht Optimierungspotenzial beim Cyberschutz

HDI Vorstand Malte Dittmann © HDI

Cyberangriffe gegen die Unternehmens-IT kleiner und mittelständischer Unternehmen gibt es täglich. Einen wirksamen Schutz gegen solche Angriffe und deren Folgen können Präventionsmaßnahmen leisten. Dazu gehören technische genauso wie organisatorische Maßnahmen oder auch solche, die Mitarbeiter für die Cyberrisiken sensibilisieren. Eine Studie der HDI Versicherung zeigt hier beträchtliches Potenzial zur Verbesserung des Cyberschutzes auf.

Die Studie zum Thema Cybersicherheit erstellte das Forschungs- und Beratungsinstitut Sirius Campus im Auftrag der HDI Versicherung. Dazu befragte das Institut Ende letzten Jahres Freiberufler sowie IT- und Versicherungs-Entscheider von mehr als 500 kleinen und mittelständischen Unternehmen (KMU). Ein Ergebnis der Studie: Viele Unternehmen können durch die Kombination von Präventionsmaßnahmen ihren Cyberschutz wirksam erhöhen.

Technische Maßnahmen an erster Stelle

Technische Maßnahmen sind die gängigsten Vorkehrungen, mit denen sich Unternehmen gegen Bedrohungen aus dem Cyber-Raum schützen. Firewalls, Spam-Schutz und automatische Datensicherungen durch Backups werden laut HDI Studie am häufigsten verwendet. So gaben 83 Prozent der Befragten an, dass sie Firewalls installiert hätten, 81 Prozent nannten Spam-Schutz und 80 Prozent automatisierte Backups. Seltener eingesetzt werden zum Beispiel Multi-Faktor Authentifizierungen (55%) oder verschlüsselte Zugänge zum Unternehmensnetzwerk zum Beispiel über VPN (66%).

Die technischen Maßnahmen haben für die Unternehmen den Vorteil, dass sie einen guten Basisschutz bieten und häufig mit einem überschaubaren Aufwand umzusetzen sind. Allerdings reichen technische Lösungen allein nicht aus. Das zeigen sowohl Untersuchungen als auch die

Schadenbilder von erfolgreichen Cyberangriffen. Organisatorische Maßnahmen und Mitarbeiterschulungen sind weitere entscheidende Bausteine.

Standards, Notfallmanagement, Mitarbeiterschulungen

Organisatorische Präventionsmaßnahmen umfassen zum Beispiel verbindliche Passwort-Standards oder Schwachstellen-Scans der IT und im weiteren Sinne auch die Vorbereitung von Notfallmaßnahmen für einen Cyberangriff. Am weitesten verbreitet (bei 72% der KMU) sind verbindliche Standards für den Umgang mit Passwörtern. Kritischer sieht es dagegen in Sachen Notfallmanagement aus. So sind die Zuständigkeiten bei einem Cyberangriff lediglich bei jedem zweiten Unternehmen (55%) eindeutig festgelegt.

Angriffe, die auf die Schwachstelle „Mensch“ zielen, sind in der Praxis am erfolgversprechendsten – für den Angreifer. „Im Rahmen der Studie wurden von betroffenen Unternehmen Angriffsmethoden wie Phishing-Mails oder Social Engineering mit Abstand am häufigsten genannt. Denn Mitarbeiter, die E-Mail-Anhänge von Unbekannten öffnen oder auf zweifelhafte Links klicken, können Kriminellen unkontrollierte Zugänge in die IT-Systeme öffnen“, stellt HDI Vorstand Malte Dittmann fest. Umso überraschender ist das Ergebnis, dass laut HDI Studie nur knapp die Hälfte (48%) der befragten Unternehmen mindestens einmal jährlich Mitarbeiterschulungen zur Cybersicherheit einsetzt. Ein Viertel (25%) der KMU testen ihre IT-Sicherheit durch simulierte E-Mailangriffe.

Kombinierte Präventionsmaßnahmen halbieren Schadenhöhe

Cyberangriffe sind vielfältig und die Schwachstellen, auf die diese zielen, immer wieder andere. Deshalb gibt es auch nicht die eine wirksame Präventionsmaßnahme, die den perfekten Schutz bietet. Die HDI Cyberstudie zeigt deutlich: Erst eine Kombination aus technischen Vorkehrungen und organisatorischen Regeln mit Maßnahmen zur Mitarbeitersensibilisierung verspricht einen möglichst wirksamen Schutz.

So waren 31 Prozent aller befragten Unternehmen in der letzten Zeit von erfolgreichen Cyberangriffen betroffen. Von denjenigen, die mehr als zehn der untersuchten Präventionsmaßnahmen einsetzen, waren es lediglich 18 Prozent. Noch signifikanter war der Unterschied bei der durchschnittlichen Schadenhöhe: Sie lag bei den 23 Prozent der befragten Unternehmen, die mehr als zehn Maßnahmen einsetzten bei 54.000 EUR – im Vergleich zu durchschnittlich 95.000 EUR bei der Betrachtung aller betroffenen KMU.

Risiko-Audits erhöhen die Informationssicherheit

Cyberrisiken sind extrem dynamisch und immer im Einzelfall zu bewerten. „Eine individuelle Beurteilung der Risiken durch ein Cyber-Sicherheitsaudit ist deshalb auch für KMU von zentraler Bedeutung“, betont HDI Vorstand Dittmann. Folgerichtig wünscht sich auch die Hälfte aller Befragten eine externe Bewertung ihrer Cyber-Risiken durch ein Audit als Zusatzleistung einer Cyberversicherung. Durch ein Audit werden mögliche Schwachstellen der IT-Infrastruktur festgestellt und potenzielle Gegenmaßnahmen aufgezeigt. Im Rahmen der Cyber-Versicherung bietet HDI mit dem „Security Baseline-Check“ daher ein Audit ihres Kooperationspartners Perseus Technologies zu vergünstigten Konditionen an.