Presseaussendung

PwC Studie: Österreichs Unternehmen nicht ausreichend auf Cyberattacken vorbereitet

- **84 Prozent der österreichischen Unternehmen haben keine umfassende IT-Sicherheitsstrategie**
- **73 Prozent verfügen über kein Mitarbeitertraining zum Thema IT-Sicherheit**
- **Schwierigkeiten bei der Täteridentifikation: Nur 14 Prozent der Befragten trauen sich zu, Cyberattacken richtig einzuordnen**

Wien, 19. Jänner 2018 – Massive Verstöße im Bereich der Cybersicherheit sind beinahe alltäglich geworden und sorgen regelmäßig für Schlagzeilen, die Konsumenten und Führungskräfte in Unruhe versetzen. Trotz der Sensibilisierung für das Thema sind viele Organisationen auf der ganzen Welt nach wie vor unsicher, wie sie in einer zunehmend digitalen Gesellschaft mit Cyber-Risiken umzugehen haben. Das zeigt die aktuelle Studie von PwC *„Global State of Information Security® Survey 2018" (GSISS)*, für die weltweit 9.500 Führungskräfte zum aktuellen Status quo befragt wurden.

Österreichs Unternehmen hinken in der Vorbereitung massiv hinterher

Mittlerweile besteht eine große Ungleichheit darin, wie unterschiedliche Länder auf Cyberattacken vorbereitet sind. Die GSISS 2018 zeigt, dass besonders Länder wie Japan (72 Prozent) und Malaysia (74 Prozent), in denen Cyberattacken als größte nationale Sicherheitsbedrohung angesehen werden, eine umfassende Informationssicherheitsstrategie vorweisen können.

Österreichs Unternehmen hinken hier allerdings enorm hinterher: 84 Prozent verfolgen keine IT-Sicherheitsstrategie. Auch die Bewusstseinsbildung der Mitarbeiter findet nicht in ausreichendem Maß statt: Nur 27 Prozent der Unternehmen verfügen über ein spezifisches Mitarbeitertrainingsprogramm. Käme es zu einer Cyberattacke, so hätten die meisten Betroffenen Schwierigkeiten, die Täter eindeutig zu identifizieren. Lediglich 14 Prozent der österreichischen Befragten vertrauen auf ihre Fähigkeit, einen Vorfall richtig einzuordnen.

„Bisher verursachten Cyberattacken nur relativ geringe Schäden, dennoch wird die destruktive Kraft solcher Angriffe immer stärker spürbar. In Österreich gibt es hier eindeutig Aufholbedarf. Unternehmen sollten ihre Sicherheitsstrategie neu überdenken und proaktiv in die Hand nehmen", so Christian Kurz, Senior Manager und Cybersicherheitsexperte bei PwC Österreich.

Cyberrisiken: Führungskräfte müssen mehr Verantwortung übernehmen

Dass es ein effizientes Kontrollsystem sowie ein proaktives Risikomanagement gibt, liegt im Verantwortungsbereich der Unternehmensleitung. Dennoch zeigt die GSISS 2018, dass lediglich 24 Prozent der Top-Manager in Österreich proaktiv an der Gestaltung einer Gesamtsicherheitsstrategie des Unternehmens mitarbeiten.

„Führungskräfte sollten jetzt die Gelegenheit nutzen und sinnvolle Maßnahmen für ihr Unternehmen in die Wege leiten. So können sie die Widerstandskraft ihrer Organisation gegenüber Cyberrisiken stärken und eine nachhaltig sichere digitale Gesellschaft schaffen", empfiehlt Kurz.

IoT als große Schwachstelle - CISO gewinnt zunehmend an Bedeutung

Parallel zum digitalen Fortschritt brauchen Organisationen entsprechende Führung und Prozesse, um die notwendigen Sicherheitsmaßnahmen umzusetzen. Viele Unternehmen stehen dabei erst am

Anfang. „Besonders die steigende Anzahl unsicherer Geräte in Verbindung mit dem ‚Internet of Things' (IoT) führt zu weitreichenden Schwachstellen bei der Cyber-Sicherheit. Zunehmende Bedrohungen der Datenintegrität könnten bewährte Systeme untergraben, kritische Infrastruktur beeinträchtigen und so zu physischen Schäden führen", warnt der PwC-Experte. „Umso wichtiger ist es, dass sich Unternehmen professioneller aufstellen. Hier gewinnt die Position des CISO immer stärker an Bedeutung."

Der Chief Information Security Officer (CISO) hat Sicherheitslücken aufzudecken und hervorzuheben, damit die Unternehmensleitung ihre Aufgabe im Hinblick auf das Verständnis für und die Auseinandersetzung mit potenziellen Risiken für das Unternehmen wahrnehmen kann.

Gebündelte Kräfte zur Risikominimierung
Um gegen Cyberattacken besser gewappnet zu sein, sind gemeinsame Anstrengungen aller Stakeholder, ein besserer Informationsaustausch sowie eine gute Koordination untereinander notwendig. Dadurch wird es möglich sein, potenzielle Risiken neuer Technologien aufzudecken. Nur knapp die Hälfte (49 Prozent) der heimischen Unternehmer gibt an, formell mit anderen Akteuren ihrer Branche, einschließlich Mitbewerbern, zusammenzuarbeiten, um Bedrohungen zu verringern.

„Glaubwürdige, zeitgerechte und verwertbare Informationen zu Cyberbedrohungen sind entscheidend für eine kurze Reaktionszeit und die Widerstandsfähigkeit eines Unternehmens", so Christian Kurz. „Um auf Cyberattacken zu reagieren, braucht es über alle Organisationen, Branchen, Regionen und Länder hinweg gemeinsame Anstrengungen, deren Effektivität von der Bereitschaft zur Zusammenarbeit abhängt."

Mehr Informationen zum Thema sowie die gesamte Studie finden Sie unter:
www.pwc.at/gsiss

Über PwC:
Vertrauen in der Gesellschaft aufbauen und wichtige Probleme lösen – das sehen wir bei PwC als unsere Aufgabe. Wir sind ein Netzwerk von Mitgliedsunternehmen in 158 Ländern. Mehr als 236.000 Mitarbeiterinnen und Mitarbeiter erbringen weltweit qualitativ hochwertige Leistungen im Bereich Wirtschaftsprüfung, Steuerberatung und Unternehmensberatung. Sagen Sie uns, was für Sie von Wert ist. Und erfahren Sie mehr auf www.pwc.at.

Weitere Informationen erhalten Sie bei:
Barbara Lang
Corporate Communication
Tel.: 01 501 88-5104
E-Mail: barbara.lang@pwc.com