Cyberattacken sind kein Schicksal:

Effizienter Schutz gegen Internetkriminalität

- **Bewusstseinsbildung für Gefahrenpotenzial ist der erste Schritt zu mehr Sicherheit**
- **Bereits einfache und kostengünstige Maßnahmen eliminieren Großteil der Bedrohungen**
- **Cybersicherheit erfordert laufende Anpassungen**

Wien, April 2017. Angriffe auf die IT-Infrastruktur gehören mittlerweile zu den größten Gefahrenquellen für österreichische Unternehmen. Das Bedrohungspotenzial reicht vom banalen Hacken einer Website bis zu massiven Störungen digitalisierter Produktionsprozesse. Während die heimischen Leitbetriebe bereits zu einem großen Teil gezielte Abwehrstrategien umsetzen, ist die Situation bei den österreichischen Unternehmen insgesamt noch nicht zufriedenstellend, wie zahlreiche Fachleute bei einer Expertenrunde der Exzellenzplattform Leitbetrieb Austria zum Thema „Cybersicherheit: Chancen nutzen, Gefahren ausschalten“ betonten. Die Veranstaltung wurde in Zusammenarbeit mit den Netzwerkpartnern Raiffeisen Landesbank NÖ-Wien und bit media e-solutions durchgeführt.

Monica Rintersbacher, Geschäftsführerin von Leitbetriebe Austria, ortet eine gefährliche Mischung aus Verdrängung und Fatalismus: „Heute sind sich zwar praktisch alle Unternehmen der Gefahren durch Cybercrime bewusst, getan wird trotzdem oft nichts. Offenbar führt mangelndes Wissen über sinnvolle Abwehrstrategien dazu, dass man mögliche Attacken auf die IT und die Datenbestände des Unternehmens geradezu als unabwendbares Schicksal hinnimmt – was es aber definitiv nicht ist.“

Schon mit technisch recht einfachen Mitteln, geringem Kostenaufwand und einer Basisschulung der Mitarbeiter in Sachen IT-Sicherheit kann viel erreicht werden: „In der Regel muss sich ein Unternehmen ja nicht gegen ganze Cyberarmeen schützen. Die reale Bedrohung geht in der Praxis viel öfter von kleineren Gruppen, gleichsam einer Art von Internet-Ladendieben, aus. Auch wenn man nur gegen diese ausreichend geschützt ist und professionelleren Angreifern Attacken zumindest erschwert, verbessert das die Sicherheitslage eines Unternehmens ganz drastisch. Der Kampf gegen Internetkriminalität muss offensiv angegangen werden, dann hat man beste Chancen, ihn auch zu gewinnen.“

Das unterstreicht auch Walter Khom, Geschäftsführer des steirischen IT-Sicherheitsspezialisten bitmedia, der bei vielen Unternehmen anhaltend mangelndes Gefahrenbewusstsein ortet. „Präventivmaßnahmen werden oft erst nach einem ersten Schadensfall gesetzt und Informationssicherheit wird der Einfachheit halber ausschließlich als Aufgabe der IT-Abteilung betrachtet. Dabei sind die meisten Sicherheitslücken eindeutig dem Faktor Mensch – Stichworte sorgloser Umgang mit Passwörtern, Phishing-Angriffe, aber auch Social Engineering – und nicht der IT zuzuordnen." Entscheidend seien daher intensive Aufklärung und Bewusstseinsbildung auf allen Ebenen. Khom: „Mittels digitaler Schulungsangebote (e-learning) ist das auch mit vertretbarem Zeit- und Kostenaufwand möglich und man kann damit effizient künftigen Schadensfällen vorbeugen."

Für Stefan Kojalek, Geschäftsführer des Aktuell Raiffeisen Versicherung-Maklerdiensts, steht eine gesamtheitliche Betrachtungsweise des Themas Cybersicherheit im Vordergrund: „Cyber-Security muss ‚Chefsache' werden. Sie ist definitiv Pflicht, nicht Kür und muss strategisch in das umfassende Risikomanagement integriert werden. Langfristig sind Investitionen in die IT-Sicherheit Investitionen in die eigene Wettbewerbsfähigkeit."

Michaela Rammel, Bereichsleiterin Firmenkunden der Raiffeisenlandesbank NÖ-Wien, sieht das Zusammenspiel moderner Sicherheitssysteme und kompetenter Anwendung als entscheidenden Faktor: „Sicherheit ist das zentrale Thema im Online-Banking. Alle Systeme zur Abwehr möglicher Bedrohungen werden daher von uns laufend ausgebaut und aktualisiert." Dennoch liege ein entscheidender Beitrag für sicheren elektronischen Zahlungsverkehr immer auch beim Kunden: „Schon mit kleinen Maßnahmen können große Beiträge für die Online-Sicherheit geleistet werden. So sollten für Online-Banking ausschließlich sichere WLAN-Netze genutzt werden und Updates für Smartphone, Tablet sowie PC immer sofort installiert werden."

Gründe, sich des Themas Cybersicherheit intensiv anzunehmen, gibt es für Unternehmen jedenfalls täglich mehr. „Die Gefahr, die vom virtuellen Raum ausgeht, wird laufend größer. Das zeigen auch die Zahlen der aktuellen Kriminalstatistik. Es gab 2016 um fast 31 Prozent mehr angezeigte Fälle als im Jahr davor", erklärt Philipp Blauensteiner vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung. Doch müssten Unternehmen das nicht als Schicksal hinnehmen, sondern auch mit vertretbaren Kosten sei effektive Vorbeugung möglich: „Auch wenn es keinen hundertprozentigen Schutz vor Angriffen gibt, kann man mit organisatorischen und technischen Maßnahmen sowie durch Bewusstseinsbildung die Widerstandsfähigkeit des Unternehmens erhöhen. Cyber-Sicherheit ist dabei kein Zustand sondern ein Prozess. Wer kontinuierlich seine ‚Hausaufgaben' erledigt, schützt sich nicht nur vor dem ‚virtuellen Ladendieb', sondern macht auch hochprofessionellen Angreifern das Leben deutlich schwerer."

Über Leitbetriebe Austria

Leitbetriebe Austria ist die Exzellenz-Plattform von durch das Leitbetriebe Institut ausgezeichneten Vorzeigebetrieben der österreichischen Wirtschaft. Mit der Mission „Gemeinsam sind wir Marke“ repräsentieren die Leitbetriebe öffentlichkeitswirksam wertorientierte Ziele wie Innovation, Wachstum, Marktstellung und Mitarbeiterentwicklung. Das Netzwerk ist ein aktives Forum von Entscheidungsträgern zum Austausch auf Augenhöhe. www.leitbetriebe.at

Pressekontakt Leitbetriebe Austria:

Thomas Brey, M&B PR; T: 01 233 01 23-15; M: 0676 542 39 09, E: brey@mb-pr.at