Pressemitteilung

Cybersecurity: Von Trojanern und Würmern – Wie sich Unternehmen vor Cyber-Attacken schützen

Cyber-Crime ist längst ein internationales Problem. Unternehmen weltweit sind von Cyber-Attacken betroffen und erleiden beachtliche finanzielle Schäden und Reputationsverluste.

Wien, 27. November 2019 - Anlässlich des Cybersecurity Breakfasts am 27. November 2019 bei Funk International Austria in Kooperation mit der Risk Management Association wurde das Thema Cyber-Crime aus den Blickwinkeln „Threats – Liability – Mitigation“ beleuchtet und diskutiert.

Aktuelle Studien belegen die steigende Anzahl an Computerkriminalität. Brigitta John, MBA, Vorstandsmitglied der Risk Management Association e.V. erläutert in ihrer Eröffnungsrede zum Funk Cyber-Breakfast: „Sieben von zehn befragten Unternehmen gaben an, von Datendiebstahl, Industriespionage oder Sabotage in den letzten zwölf Monaten betroffen gewesen zu sein. Enorme Kosten entstehen aufgrund von Imageschäden, Patentrechtsverletzungen, Betriebsunterbrechungen sowie Ermittlungs- und Aufklärungskosten, wovon kleine und mittelständische Unternehmen nicht verschont bleiben.“

Um die Angriffsfläche von Unternehmen für Cyber-Angriffe so gering wie möglich zu halten, ist ein ausgeklügeltes Sicherheits- sowie Managementsystem erforderlich. Letztendlich trägt die Geschäftsführung die volle Verantwortung und haftet sowohl nach innen als auch nach außen.

Rechtsanwalt Dr. Franz Althuber ergänzt: „Die Einrichtung einer risiko- und unternehmensadäquaten IT gehört zu den Kernpflichten der Geschäftsführung. Auch und gerade bei Cyber-Attacken, bei denen mitunter Schäden in Millionenhöhe entstehen, kann fehlerhaftes Compliance-Management zu Schadenersatzansprüchen gegenüber den Leitungsorganen führen.“

Mario Heinisch, CEO von Funk International Austria erläutert in seinem Vortrag, warum eine Cyber-Versicherung in der heutigen Zeit nicht mehr wegzudenken ist: „Im Umgang mit Cyber-Risiken haben wir zwei Möglichkeiten: Die aktive und die passive Risikobewältigung. Bei der aktiven Risikobewältigung geht es um technische und organisatorische Maßnahmen bis hin zur Notfallplanung. Ab einem gewissen Punkt macht es aber auch Sinn, über einen Risikotransfer in eine Cyber-Versicherungslösung nachzudenken: der passiven Risikobewältigung. Wir sehen eine Cyber-Versicherung nicht als Alternative für sehr gute IT-Sicherheitsmaßnahmen sondern als betriebswirtschaftliche Ergänzung ab einem bestimmten IT-Sicherheitsniveau."

"Cyber-Versicherungen helfen Firmen und Organisationen ihre Digitalisierungsrisiken abzufedern", betonte der Sicherheitsexperte und Unternehmensberater Dr. Cornelius Granig beim Cyber Breakfast von Funk International Austria. Dazu ist es notwendig, dass Geschäftsführer und verantwortliche Manager die Sicherheit der Systeme und Prozesse ihrer Organisationen nachhaltig analysieren und ggf. auch Verbesserungen und Updates durchführen.

"Die Herstellung der Versicherbarkeit und die Diskussion über die möglichen Inhalte einer Cyber-Polizze lösen üblicherweise einen wichtigen Nachdenk- und Erneuerungsprozess aus, der sehr wesentliche Impulse für die Risikominimierung gibt. Die Produkte der Cyber-Versicherungen sind ein großes neues Wachstumsfeld und stellen einen wichtigen Bestandteil jeder unternehmensweiten Cyber-Security Strategie dar”, sagt Dr. Granig, der früher selbst im Vorstand eines großen Versicherungsunternehmens tätig war. Ein Komplettschutz vor Cyber-Attacken existiert nicht – das Risiko muss aber in jedem Fall festgestellt und das Restrisiko abgesichert werden.