Digitalisierung sicher gestalten

Die Corona-Pandemie hat die Digitalisierung vorangetrieben. Unternehmen müssen im Falle eines Angriffs ihre Funktionsfähigkeit erhalten. Dazu bedarf es der Zusammenarbeit von Behörden und Unternehmen.

Die Digitalisierung hat uns in vielen Bereichen geholfen, die Corona-Krise besser zu bewältigen. Das hat uns aber auch gezeigt, wie wichtig gerade jetzt der Schutz der digitalen Dienste vor Angriffen ist“, sagte der Generalsekretär im Innenministerium, Mag. Helmut Tomac, beim Sicherheitsforum Digitale Wirtschaft am 4. September 2020 im Bundesministerium für Inneres (BMI). „Zusammenarbeit ist dabei das effizienteste und effektivste Mittel. Deshalb freut es mich, dass wir das Kuratorium Sicheres Österreich und sein Sicherheitsforum als Partner bei dieser Aufgabe an Bord haben.“

Zusammenarbeit forcieren. Das Innenministerium ist für die Wirtschaft einer der wichtigsten Ansprechpartner, wenn es um die staatlich-private Zusammenarbeit in puncto Cyber-Sicherheit geht. Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) ist mit dem Cyber-Security-Center (CSC) und seiner Vorreiterrolle bei der Umsetzung des NIS-Gesetzes ein wesentlicher Kontakt zu den staatlichen Cyber-Sicherheitsakteuren. Die Teilnehmerinnen und Teilnehmer am Forum haben zum Ausdruck gebracht, dass diese wichtige Thematik noch breiter in die Wirtschaft transportiert werden müsse. Speziell Klein- und Mittelbetriebe müssten stärker einbezogen und mit Know-how versorgt werden, damit sie sich besser vor Cyber-Angriffen schützen können.

Digitale Sicherheit ist nicht mit Cyber-Sicherheit gleichzusetzen. Während Cyber-Sicherheit vorrangig den Schutz vor und die Abwehr von Angriffen über den Cyber-Raum abdeckt, steht bei digitaler Sicherheit die vorbeugende Wirkung von rechtlichen, organisatorischen und technischen Maßnahmen im Vordergrund – etwa, wie aus sicherheitstechnischer Sicht damit umgegangen werden soll, dass immer mehr Geräte mit einem Internetzugang ausgestattet sind. Oder wie bei der Entwicklung neuer Geräte und Programme von vornherein schon auf mehr Sicherheit geachtet werden kann – Stichwort „Security by Design“. Viele Bereiche unseres täglichen Lebens würden sich immer weiter in die digitale Welt verlagern, sagte Tomac. „Auf der einen Seite macht diese Entwicklung viele Vorgänge schneller, einfacher und effizienter. Auf der anderen Seite bietet sie Angriffsfläche für neue Arten der Kriminalität sowie Sicherheitslücken, die es zuvor nicht zu beachten gab“, sagte der Generalsekretär.

Helmut Tomac: „Wir setzen noch stärker auf Prävention, Ausbildung und Kooperation, damit Cyber-Angriffe verhindert und nicht nur verfolgt werden.“

Erwin Hameseder: „Damit die Digitalisierung zu einem Hilfsmittel und nicht zu einem Risiko wird, müssen wir sie von Beginn an sicher gestalten.“

Mehr Kriminalität im Netz. Die Zahl der angezeigten Delikte betreffend Internetkriminalität ist in den vergangenen zehn Jahren um mehr als das Sechsfache (2010: 4.223, 2019: 28.439 Anzeigen) angestiegen. Eine große Anzahl von Datenlecks in den Jahren 2018 und 2019 hatten zur Folge, dass massenhaft personenbezogene Daten im Internet veröffentlicht oder im Darknet zum Kauf angeboten wurden. Täter konnten so illegal Zugangsdaten erlangen, die sie wiederum für Hacking und widerrechtliche Zugriffe auf Computersysteme genutzt haben. 684 derartige Fälle wurden 2019 registriert, was eine Zunahme von 281 Fällen innerhalb eines Jahres bedeutet – 2018 waren es 403 Anzeigen. „Diese Entwicklung zeigt ganz klar: Hier gibt es Aufholbedarf, vor allem auch in puncto Prävention. Mit dem KSÖ gibt es das perfekte Forum, um dieser Problemstellung gemeinsam entgegenzuwirken. Denn der Schutz der Digitalisierung kann nur gemeinsam gelingen“, bekräftigte Tomac.

Steigende Gefahr für Unternehmen. Österreichische Klein- und Mittelbetriebe, als Nischen-Player, haben wertvolles geistiges Eigentum geschaffen. Dieses Wissen ist von internationalem Interesse. „Unternehmen brauchen die Fähigkeit der Cyber-Resilienz: Trotz widriger Umstände, kontinuierlich ihre Leistung zu liefern“, erklärte DI (FH) Robert Lamprecht, Direktor des Wirtschaftsprüfungs- und Beratungsunternehmens *KPMG Austria*. Die Cyber-Sicherheitsstudie 2020, die *KPMG* in Zusammenarbeit mit dem *KSÖ* und dem *Sicherheitsforum Digitale Wirtschaft* Österreich erstellt hat, gibt Aufschluss darüber, dass Cyber-Kriminalität für Unternehmen weltweit immer gefährlicher wird.

Ein nicht zu unterschätzender Risikofaktor, den die Studie thematisiert, bilden staatlich unterstützte Cyber-Angriffe – die institutionalisierte Kriminalität durch staatliche Stellen. Diese gezielten Angriffe, im Fachjargon als „Advanced Persistent Threats“ bezeichnet, machen sich auch in Österreich bemerkbar. *KSÖ*-Experten stufen staatlich unterstützte Angriffe in einer Cybersecurity-Risikomatrix als eine der größten Gefahren im Cyber-Sicherheitsbereich ein. Viele heimische Unternehmen würden laut Studie diese Gefahr verkennen. Unternehmen, die Weltmarkt- oder Branchenführer sind oder innovative Ideen haben. Die Rolle der Cyber-Sicherheit müsse zudem neu definiert werden, als synergieschöpfendes Element, um die eigentliche Funktion eines Unternehmens zu erhalten und zu gewährleisten, auch wenn Unvorhergesehenes passiert. Unternehmen brauchen

Fotos: Gerd Pachauer

Sicherheitsforum Digitale Wirtschaft: Vertreterinnen und Vertreter von Behörden und der Wirtschaft diskutierten Sicherheitsfragen in Zusammenhang mit der zunehmenden Digitalisierung der Gesellschaft.

die Fähigkeit, bei Angriffen betriebs- und funktionsfähig zu bleiben.

Angriffe auf heimische Unternehmen. Die diesjährige KPMG-Studie *(https://publikationen.kpmg.at/cybersecurity-2020)* befasst sich mit der Frage, wie österreichische Unternehmen den neuen Herausforderungen der Cyberkriminalität begegnen und welche Cyber-Sicherheitsmaßnahmen getroffen werden. Die Umfrage zur Studie wurde unter 652 Unternehmen durchgeführt. Darunter Klein- und Mittelbetriebe wie auch große Unternehmen aus den Branchen Technologie, Banken, Industrie, Energiewirtschaft, Bauwirtschaft und Immobilien oder Transport, um einige davon zu nennen. Mehr als die Hälfte der Unternehmen hat technische und organisatorische Maßnahmen definiert, um für einen möglichen Angriff vorbereitet zu sein. Laut Studie würden Unternehmen zwar in die Abwehr von Cyber-Attacken investieren, jedoch die Schadensminimierung vernachlässigen.

Cyber-Versicherungen. Die Nachfrage nach Cyber-Versicherungen nehme in Österreich nur schleppend zu. Nicht einmal ein Viertel der Unternehmen besitzt eine Versicherung gegen Cyber-Angriffe. 57 Prozent der Unternehmen waren innerhalb der letzten 12 Monate – vor der Umfrage, die zwischen Februar und März 2020 durchgeführt wurde – von Angriffen aus dem Netz betroffen. 74 Prozent der Angriffe waren Phishing-Attacken.

Bewusstsein schaffen. „Damit die Digitalisierung zu einem Hilfsmittel und nicht zu einem Risiko wird, müssen wir darauf achten, sie von Beginn an sicher zu gestalten“, sagte *KSÖ*-Präsident Mag. Erwin Hameseder. „Wir treten dafür ein, dass Hard- und Software sicher sein muss und mehr unternommen wird, damit die Anwender sich darauf verlassen können.“ Das beginne bei der Ausbildung und der Schaffung von Bewusstsein für mögliche Gefahren und ende bei der Zertifizierung von digitalen Geräten, wie sie mit dem EU-Cybersecurity-Act geplant sei, erläuterte *KSÖ*-Generalsekretär Alexander Janda. „5G, künstliche Intelligenz oder das Internet of Things abzusichern, ist eine Herausforderung, die niemand alleine bewältigen kann. Die Teilnehmerinnen und Teilnehmer am Sicherheitsforum unterstützen sich daher gegenseitig und helfen anderen dabei, Antworten zu diesen Themen zu finden.“

Generalsekretär Tomac rief in Erinnerung, dass das Internet kein rechtsfreier Raum sei. „Wir setzen noch stärker auf Prävention, Ausbildung und Kooperation, damit Cyber-Angriffe verhindert und nicht nur verfolgt werden. Die Wirtschaft muss dabei einen noch größeren Teil der Verantwortung übernehmen, sonst wird es nicht möglich sein, die Österreicherinnen und Österreicher vor kriminellen Kräften im Internet zu schützen. Dass sie bereit ist, das zu tun, hat mir die heutige Diskussion mit dem KSÖ-Sicherheitsforum bestätigt.“

Das Sicherheitsforum „Digitale Wirtschaft“ organisiert regelmäßige (virtuelle) Veranstaltungen mit nationalen und internationalen Gastrednern aus Wirtschaft, Politik und Forschung zur Förderung des Informationsaustausches zu aktuellen Trends und Risikofaktoren. Es ist eine Arbeitsplattform, in der Wirtschaft, Forschung und Behörden gemeinsam Verantwortung übernehmen und ihren Beitrag zur sicheren Digitalisierung in Österreich leisten – die gegenseitige Unterstützung geht dabei über die Branchen-Grenzen hinaus. Mit der Einbindung von Expertinnen und Experten aus dem strategischen sowie technischen Bereich bildet das Forum die Basis für eine sichere Digitalisierung des Wirtschaftsstandorts Österreich.

Teilnehmende Unternehmen am Sicherheitsforum sind *A1 Telekom Austria AG, ÖAMTC, Raiffeisen Informatik GmbH, KPMG Security Services GmbH, Österreichische Staatsdruckerei, Flughafen Wien, Österreichische Lotterien, Siemens Aktiengesellschaft Österreich, Raiffeisen Bank International AG* und *UNIQA Österreich Versicherungen AG*. *Gernot Burkert*

FOTO: GERD PACHAUER