Cybercrime: Durch die zunehmende Digitalisierung von Unternehmen steigt die Anfälligkeit für Cyber-Attacken.

Innentäter: Viele Straftaten in Unternehmen werden von unzufriedenen oder gekündigten Mitarbeitern begangen.

Wirtschaft, Staat, privat

Expertinnen und Experten referierten bei der *ACIPSS*-Tagung unter anderem über Bedrohungsanalysen, Schutzziele bei Sicherheitssystemen und grenzüberschreitenden Zugang zu elektronischen Beweismitteln.

Die 30. Tagung des Grazer *Austrian Center for Intelligence, Propaganda & Security Studies (ACIPSS)* fand am 7. Februar 2020 zum zweiten Mal an der FH Campus Wien in Kooperation mit dem Fachbereich für Risiko- und Sicherheitsmanagement sowie dem *Verband der akademischen Sicherheitsberater Österreichs (VAS-BÖ)* statt. Das Generalthema lautete „Bedrohungslagen: Wirtschaft – Staat – Privat".

Regierungsprogramm. DI (FH) Mag. Thomas Goiser, Unternehmensberater und *ACIPSS*-Repräsentant Wiens, beleuchtete unter dem Titel „Aus Verantwortung für Österreich" einige Aspekte des neuen österreichischen Regierungsprogramms 2020-2024 aus Sicht des „unternehmerischen Risiko- und Sicherheitsmanagements". Einzelne Bereiche, wie z. B. Informationssicherheit, deren Gewährleistung durch die Abschaffung der Amtsverschwiegenheit bzw. des Amtsgeheimnisses erfolgen sollte, bestanden bereits in dieser Form. Auch mit der im Regierungsprogramm erwähnten Einschränkung des Informationsrechts, „soweit und solange die Geheimhaltung erforderlich und verhältnismäßig" oder „im Interesse der nationalen Sicherheit, der umfassenden Landesverteidigung oder der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit" ist, gebe es faktisch wenige Veränderungen zu erwarten. Goiser griff die Frage auf, warum ausgerechnet in „allen Justizanstalten" eine Gewährleistung der notwendigen und zeitgemäßen Sicherheitsstandards betreffend die Sicherheit öffentlich Bediensteter durch bauliche und technische Maßnahmen (u. a. Drohnenabwehr, Mobilfunkblockaden, Körperscanner, Videoanalyse und Maßnahmen zur Prävention von gefährlichem Verhalten) erforderlich sei und warum nicht auch andere Bereiche von diesen Maßnahmen erfasst werden sollten, wie z. B. das Parlament oder Gerichte. Im Regierungsprogramm würden Pläne erstellt, die als „Masterpläne" gelten, allerdings keine weiteren Hinweise enthielten, wie sie wann und wo und vor allem von wem umgesetzt werden.

Als Beispiele führte Goiser die Punkte „Katastrophenschutz" und „Strafrecht" an. Im Katastrophenschutz soll ein digitaler Zivilschutz-Probealarm eingeführt werden unter Einbeziehung der Zivilbevölkerung per Social Media, SMS, WhatsApp usw. Diese Dienste seien nicht verfügbar, sobald die Kommunikationsnetze versagen. Im Strafrecht sei die Erweiterung bzw. Präzisierung vorhandener Straftatbestände zur Bekämpfung aller Arten von Cyber-Kriminalität vorgesehen, während die Ausstattung der Behörden unerwähnt bleibe.

Bedrohungsanalysen. Im Vortrag von Dr. Beatrice Preßl und Dr. Yvonne Prinzellner zum Thema „Social Media – eine Sekundärquelle für Bedrohungsanalysen im Security Management?" ging es um die Durchführung von Bedrohungsanalysen im beruflichen Umfeld, wobei die Ergebnisse des einjährigen Forschungsprojekts vorgestellt wurden.

Das Forschungsprojekt „The Role of Social Media Analysis in Security Management" (SMASM) bestand darin, die Erstellung von Bedrohungsanalysen zu untersuchen, die von Security-Managerinnen und -Managern in Deutschland, Österreich und der Schweiz durchgeführt wurden. Einer der Schwerpunkte lag in der Analyse sozialer Medien als Informationsquelle und der Einsatzgebiete innerhalb der Unternehmenssicherheit sowie deren Vor- und Nachteile, wobei Security-Managerinnen und -Manager für die Evaluierung qualitativ und quantitativ befragt wurden. Im Zuge der qualitativen Befragung wurden zwei Arten von Bedrohungsanalysen herausgearbeitet: Ad-hoc-Analysen und statische Analysen.

Ad-hoc-Analysen – Beispiel: Es gibt einen Messerangriff in London; ein Security Manager eines deutschen Unternehmens wird per Analysetool darüber informiert. Der Security-Manager muss schnell an Informationen kommen, um Fragen wie: „Was ist passiert?" und „Haben wir Mitarbeiter in London?" zu beantworten. Die Situation muss

Fotos: Thatree/Stock.adobe.com, WBullRun/Stock.adobe.com

ACIPSS-Tagung: Maximilian Schubert, Günther Neukamp, Beatrice Preßl, Yvonne Prinzellner, Paul Schliefsteiner, Thomas Goiser.

schnell erfasst werden, damit Entscheidungen für das Unternehmen und seine Bediensteten getroffen und Maßnahmen gesetzt werden können. Soziale Medien werden in diesem Fall als Informationsquelle verwendet, weil der Zeitfaktor eine erhebliche Rolle spielt. Diese Arbeitsweise kann sich mit „quick and dirty" umschreiben lassen.

Bei statischen Analysen, die schriftlich und strukturiert ablaufen, hat man im Vergleich mehrere Wochen bzw. Monate für deren Erstellung Zeit. Die Verwendung von sozialen Medien ist zwar möglich, jedoch stehen andere Informationsquellen im Vordergrund. Hier wurde als Beispiel die Planung der Durchführung einer Veranstaltung im beliebigen Land X angeführt, wobei man schon im Vorfeld Informationen über die soziale Lage, Bedrohungen etc. sammelt, um ein genaues Lagebild zu erstellen. Man sollte stets beachten, dass Daten von sozialen Medien zu filtern und zu verarbeiten sind: Laut Experten fallen Analysen hier unterschiedlich aus (z. B. manuell, automatisiert). Den Analysten kommt große Verantwortung zu, da sie unterscheiden müssen, ob die gesammelten Informationen relevant oder irrelevant sind. Es gibt zwar Social-Media-Analysis-Tools, allerdings müssen die gesammelten Informationen am Ende „richtig" analysiert werden, wobei komplexere Tools die künftige Analysearbeit erheblich reduzieren könnten.

Fazit des Forschungsprojekts ist, dass Analysen basierend auf sozialen Medien sowohl Chancen als auch Risiken aufweisen. Soziale Medien sind wichtige Informationsquellen für Echtzeitanalysen (z. B. bei Reisesicherheit, Veranstaltungssicherheit) und werden im Sicherheitsbereich vor allem als Sekundärquellen verwendet.

Schutzziele. Der Vortrag von Ing. Günther Neukamp, CEO Senior Risk Advisor von *Neukamp & Partner Risk Consulting GmbH,* behandelte das Thema „Corporate Risk Management – Konkrete Bedrohungslage 2020". Dabei wurden unterschiedliche Schutzziele in Bezug auf Sicherheitssysteme hervorgehoben. Durch die immer stärkere Digitalisierung und den Trend in Richtung „Smart Enterprise" und „Smart Office" mit Hilfe von künstlicher Intelligenz, stärkerer Vernetzung, Prozessautomatisierungen und dem damit verbundenen Einsatz von mobilen Endgeräten wird die Situation innerhalb einzelner Unternehmen stets komplexer, da die Anfälligkeit für Cyber-Attacken höher wird. Die Innovation selbst steht im Vordergrund, wobei die Sicherheit oft vernachlässigt wird.

Schutzziele werden als Grundlage für die Erstellung von Analysen verwendet. Schutzziele für Unternehmen unterscheiden sich durch die jeweilige Perspektive: Loss Prevention, Schutz kritischer Infrastruktur, Abwehr von Industriespionage, Schutz personenbezogener Daten usw. Die wenigsten Unternehmen haben einen ganzheitlichen Überblick über ihre Schutzziele. Abgesehen von den Schutzzielen ist die Bedrohung aus unternehmens- und kontextspezifischer Sicht unterschiedlich. Allgemein kann man die steigende Systemkomplexität als Schwachstelle neuartiger Bedrohungen sehen. Unzufriedene oder gekündigte Mitarbeiterinnen oder Mitarbeiter stellen eine immense Bedrohung für Unternehmen dar. Bei zahlreichen Verbrechen in Unternehmen gibt es interne Täter oder Beitragstäterschaften im Umfang von fast 50 Prozent. Allgemein kann man eine Verlagerung der Kriminalität ins Internet verfolgen.

Elektronische Beweismittel. Dr. Maximilian Schubert, LL.M., Generalsekretär des Branchenverbandes *Internet Service Providers Austria (ISPA),* sprach über die „Die Zukunft des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln" und den damit einhergehenden praktischen Herausforderungen. Die Bedeutung elektronischer Beweismittel innerhalb der Strafverfolgung in Europa ist groß. Bei einem Großteil der strafrechtlichen Ermittlungen wird auf elektronische Daten – insbesondere Daten, die bei der Nutzung diverser Kommunikationsdienste (E-Mail, Access-Dienste etc.) entstehen – zurückgegriffen. Das nationale Strafrecht stößt dabei auf Herausforderungen, sofern der Sitz des Diensteanbieters oder der Ort der Datenspeicherung vom Sitz der Strafverfolgungsbehörde abweicht. In solchen Fällen ist ein grenzüberschreitender Zugang zu Beweismitteln erforderlich.

Drei Möglichkeiten gab es bisher für eine grenzüberschreitende Kooperation: Die Sicherstellung des Endgeräts mit direktem Zugriff auf die Daten; Rechtshilfeersuchen, die in internationalen Verträgen („Mutual Legal Assistance Treaties" – MLATs) geregelt sind, sowie ausschließlich in Bezug auf US-Provider die freiwillige Beauskunftung der Daten („voluntary disclosure"). Für Letztere ist es jedoch erforderlich, dass eine Auskunft unter Wahrung der Verhältnismäßigkeit erfolgt. Hierfür prüft das angefragte Unternehmen unter anderem, ob es eine Rechtsgrundlage für eine Auskunft nach dem nationalen Recht der anfragenden Behörde gibt. Darüber hinaus sind solche Anfragen auf einfache Vertragsdaten sowie Verkehrsdaten beschränkt, eine Anfrage von Inhaltsdaten ist auf diese Art nicht möglich und muss über Rechtshilfeersuchen erfolgen. Das Problem bei Rechtshilfeersuchen ist allerdings, dass

Foto: David Jaklin

die Beantwortungszeit, speziell bei Fällen, die keinen Notfall darstellen, oft ein bis 24 Monate beträgt.

Freiwillige Beauskunftung. Weiters gibt es im Zusammenhang mit der freiwilligen Beauskunftung Herausforderungen:
• ist es unklar, an welche Kontaktadresse sich Behörden wenden sollen;
• ist es unklar, welche Daten angefordert werden können;
• weiß man nicht, wie die Anfrage übertragen werden soll (online Plattform, Fax, E-Mail);
• wird die Anfrage in einer anderen Sprache als der am Sitz des Unternehmens gestellt;
• werden formale Anforderungen seitens der anfragenden Behörde nicht eingehalten;
• werden seitens der anfragenden Behörde nicht die notwendigen Informationen bekannt gegeben, z. B. keine gültige Rechtslage oder fehlender Gerichtsbeschluss.

Behördenanfragen. Während Behördenanfragen an US-Provider aus anderen EU-Staaten bis zu 80 Prozent positiv beantwortet werden können, lag Österreich hier gemäß einer Statistik von Europol für 2018 unter dem EU-Durchschnitt von 66 Prozent. Um hier an das europäische Spitzenfeld aufzuschließen, wurden die Vorteile eines „Single Point of Contact“ (SPOC) hervorgehoben: Dieser kombiniert effizient das notwendige rechtliche und technische Fachwissen. Länder mit SPOCs haben nachweislich höhere Erfolgsraten bei Beauskunftungen, verbesserte Transparenz und weisen generell eine Qualitätssteigerung auf.

Für die Zukunft des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln werden derzeit Gesetzesvorhaben sowohl auf EU-Ebene als auch auf internationaler Ebene verhandelt, die direkte grenzüberschreitende Anordnungen vorsehen. Angesichts einer derart gravierenden Abkehr vom bisherigen Prinzip der territorial beschränkten Strafverfolgung ist Rechtssicherheit für die betroffenen Unternehmen eine Grundvoraussetzung für die effektive Zusammenarbeit zwischen Behörden und Unternehmen. Daher gilt es, die Behörden im angefragten Staat jedenfalls auch weiterhin in das Verfahren zu involvieren. *N. F. A*