Produktpräsentation beim Symposium Sicherheit in Wien: Offline-Schlösser und handliche Satellitentelefone

Krisen und Cybercrime

Krisenbewältigung und Cybercrime waren die Hauptthemen des 28. Symposiums Sicherheit der Erste Group am 11. und 12. Oktober 2022 in Wien.

Sicherheitsverantwortliche von Geldinstituten und aus deren Umfeld kamen am 11. und 12. Oktober 2022 im *Erste-Campus* in Wien zum 28. *Symposium Sicherheit* der *Erste Group* zusammen. In 13 Vorträgen wurden Fragen des Notfalls- und Krisenmanagements, der Business Continuity, der physischen und Informationssicherheit, des Daten- und des Arbeitnehmerschutzes erörtert mit dem Ziel, Entwicklungen aufzuzeigen und Handlungsempfehlungen herauszuarbeiten.

Krise. „Nicht alles, was man gemeinhin als Krise bezeichnet, ist auch eine", rückte Ing. Karl Weißl, Erste Group, Begriffe zurecht. Eine Krise kommt unerwartet und ist etwas, das man vorher nicht gehabt hat und das mit dem herkömmlichen Instrumentarium nicht bewältigt werden kann. Wenn die Dinge nicht mehr im eigenen Einflussbereich liegen, wächst sich die Krise zur Katastrophe aus.

Ein Blackout (weitreichender, überregionaler Stromausfall) wäre ein solcher Fall, wobei eine bloße Strommangellage (Stromausfall für 24 bis 36 Stunden, unterbrochen von gelegentlichen Aufschaltungen) noch nicht unter diesen Begriff fällt. Unternehmen werden sich im Katastrophenfall auf ihre vitalen Funktionen zurückziehen müssen; Banken beispielsweise auf die Aufrechterhaltung des Zahlungsverkehrs (Daueraufträge, Einzüge) und die Bargeldversorgung. Diese könnte allenfalls über mobile Ausgabestellen erfolgen. Sollte das Telekommunikationsnetz zusammenbrechen, könnte auf Satellitentelefonie zurückgegriffen werden.

Krisenmanagement – BCM. „Katastrophen sind normal; Risiko gehört zum Leben", postulierte FH-Prof. DI Dr. Martin Langer, FH Campus Wien. Am sichersten kommt man zur nächsten Katastrophe, wenn man Systeme für sicher erklärt, niemanden von Mängeln informiert, bagatellisiert, vertuscht, Schuldige sucht und bestraft, aber nichts ändert. Frei nach Murphy: Wenn eine Möglichkeit zur Katastrophe führt, wird diese auch eintreten.

Nach der *High-Reliability-Organization*-Theorie *(HRO)* sei es möglich, durch Planung und Antizipation das Unerwartete zu managen. Wenn dieses Unerwartete sprachlich erfasst und benannt werden kann, kommt man auch zur Problemlösung (Rumpelstilzchen-Effekt). Auszugehen sei davon, „das Schlechteste zu planen, aber das Beste zu hoffen".

Dr. Klaus Bockslaff von der *Verismo GmbH (verismo.ch)* bezeichnete den BSI-Standard 200-4 als praxisnahe Anleitung, um ein *Business-Continuity-Management*-System *(BCM)* in der eigenen Institution zu etablieren. In den nächsten Monaten ist mit der Publizierung der *ISO FDIS 22361* zu rechnen. Diese internationale Norm enthält Leitlinien für das Krisenmanagement, die Organisationen dabei helfen sollen, ihre Fähigkeit zum strategischen Krisenmanagement zu planen, einzurichten, aufrechtzuerhalten, zu überprüfen und ständig zu verbessern. Das Thema Krisenmanagement wird darin umfassend geregelt und wird für Organisationen aller Größenordnungen anwendbar sein. Die Norm ist strategisch ausgerichtet; zwischen Krisen- und Ereignismanagement wird klar unterschieden.

Dem klassischen BCM stellte Marco Felsberger, *Resilience Engineers GmbH,* die *Adaptive Business Continuity* gegenüber. Das System bewegt sich im Bereich zwischen Komplexität (Vorhersagen sind noch möglich) und Chaos mit dem Ziel einer kontinuierlichen Fortführung der Geschäftstätigkeit nach einer unerwarteten Nichtverfügbarkeit von Personen, Gebäuden und Ressourcen.

Einen Einblick in praktisch gelebtes Krisenmanagement gaben Eva-Maria Altmann, MSc, und Florian Polt, MA, von der *Uniqa*-Versicherung. Das Unternehmen war mit Personal und Vermögenswerten in der Ukraine vertreten und vom Kriegsausbruch am 24. Februar 2022 betroffen. Bemerkenswert war dabei, dass diesbezügliche Anzeichen wie Räumung von Botschaften, schon einen Monat vorher zu erkennen waren, was unternehmensintern zu ersten Maßnahmen und einer gesamthaften Risikoanalyse geführt hat. Bereits am 3. Februar wurden auf allen Ebenen Präventionsmaßnahmen umgesetzt. Bei Kriegsausbruch wurde das Krisenteam aktiviert, das in weiterer Folge, aufgeteilt in

Fotos: Kurt Hickisch

die Bereiche IT, Finanz und Mitarbeiter/-innen-Schutz und -fürsorge, die entsprechenden Maßnahmen getroffen und innerhalb von zwei Monaten abgeschlossen hatte.

Schutz KRITIS. Ministerialrat Jürgen Dachauer, MA, *Direktion für Staatsschutz und Nachrichtendienst,* erläuterte die Maßnahmen, die vom BMI zum Schutz von Unternehmen der kritischen Infrastruktur getroffen werden. Zurückgehend auf die RL 2008/114/EG des Rates, wurde von der Bundesregierung das Programm zum Schutz kritischer Infrastrukturen (Masterplan APCIP 2014) beschlossen, der in 12 Sektoren etwa 400 Unternehmen der kritischen Infrastruktur umfasst. Für diese Unternehmen wurde unter anderem ein Frühwarnsystem eingerichtet. In Kürze wird allerdings die zum Zeitpunkt des Referats bereits in der finalen Fassung vorliegende RL des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen (RKL-RL) in Kraft treten, die dann innerhalb von 21 Monaten umzusetzen sein wird. Die Mitgliedstaaten werden verpflichtet, Maßnahmen zu ergreifen, die für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten wesentlich sind. In Hinkunft werden mehrere 1.000 Unternehmen in 11 Sektoren erfasst sein.

Eigentumskriminalität. „Wenn ältere Herrschaften, die üblicherweise Beträge um die 1.000 Euro abheben, plötzlich hohe Geldbeträge abheben oder das Schließfach leerräumen wollen, könnten sie Opfer von Kautionsbetrügern geworden sein", machten Jörg Kohlhofer und Josef Janisch von der Landespolizeidirektion Wien auf ein von den Schadenssummen her massives Problem aufmerksam. Bankangestellte sollten in solchen Fällen nachfragen, ob etwas passiert sei, dadurch ins Gespräch mit den potenziellen Opfern kommen und die Polizei verständigen. Die Täter wählen aus dem Telefonbuch Personen aus, deren Vornamen auf ein höheres Alter schließen lassen. Der Anrufer gibt sich als Polizist aus, der von der Festnahme eines nahen Angehörigen wegen einer Straftat berichtet, wobei eine weitere Haft durch die Stellung einer Kaution in fünfstelliger Höhe vermieden werden könne. Bei einem schweren Verkehrsunfall in Graz wurden die ersten Anrufe dieser Art schon nach vier Stunden getätigt. Das Geld oder entsprechende Vermögenswerte würden abgeholt. In einem Fall mit einer Schadenssumme von 200.000 Euro wurde wegen Infektionsgefahr verlangt, das Geld in einer Schachtel vor die Haustür zu stellen, von wo es abgeholt wurde. Mitunter werden die Opfer mit einem bestellten Taxi zur Bank gefahren, wobei die Täter bestrebt sind, den telefonischen Kontakt zum Opfer nicht abreißen zu lassen. Das hinter diesen Aktionen stehende Mastermind ist laut den Beamten namentlich bekannt, jedoch für die österreichische Justiz nicht greifbar.

Referenten beim Symposium Sicherheit: Philipp Mattes-Draxler, Marco Felsberger, Karl Weißl, Teresa Allum

Die Schadensfälle durch Cybercrime in Österreich steigen stetig an. 2020 wurden 35.915 Fälle in der Statistik erfasst. In vielen Fällen reicht es, den Hausverstand einzusetzen und sich zu fragen, warum gerade ich kontaktiert werde. Keine Finanzdaten preisgeben. Sichere Passwörter sollten 20 Zeichen umfassen, die aus den Anfangsbuchstaben der Worte eines Merksatzes gebildet werden können. Aus einem „i" könnte dabei eine „1" werden. Die letzten Buchstaben könnten, so der Rat der Experten, den Bereich bezeichnen, für den das Passwort verwendet wird, also etwa *.finanz, .büro, .privat*. In öffentlichen WLANs sollten keine sensiblen Daten versendet und sollte auf Onlinebanking und -shopping verzichtet werden. Der *CEO Fraud* ist eine Betrugsform, bei dem die Täter über eine manipulierte E-Mail-Adresse, die der des Chefs gleicht oder ähnlich sieht, überweisungsbefugte Mitarbeiter kontaktieren. In der E-Mail wird der dringliche Transfer eines Geldbetrags auf ausländische Konten, meist in China oder Hong Kong, gefordert. Um dem *CEO-Fraud* vorzubeugen, empfiehlt es sich, mit dem Chef, dessen Abwesenheit von den Tätern ausgenützt wird, ein Codewort zu vereinbaren, um sicher zu gehen, dass die angeblich so dringende Geldüberweisung tatsächlich von ihm ausgeht.

Im Internet sollten keine intimen Details preisgeben werden. *Sextortion* ist eine Form der Erpressung, bei der der Täter den Opfern mit der Veröffentlichung von Nacktfotos oder -videos des Opfers droht, wenn sie nicht eine bestimmte Summe zahlen. Sollte man den Verdacht haben, dass Schadsoftware auf das Gerät geladen wird: Netzstecker ziehen bzw. beim Handy den Flugmodus aktivieren, damit die Verbindung unterbrochen wird.

Warum die Täter so großen Druck auf die telefonisch kontaktierten Opfer ausüben, erklärte Teresa Allum, MSc, *VASBÖ,* psychologisch damit, dass ihnen nicht Zeit gegeben werden soll nachzudenken. Im Denken des Opfers sollen Automatismen ablaufen, wie etwa beim Autofahren, wo auch nicht jeder Handgriff überlegt wird.

Cyber-Kriminalität. Als die beiden größten Player im Geschäft mit Ransomware, die den Markt großteils beherrschen, bezeichnete Philipp Mattes-Draxler, *PwC Austria,* die Organisationen *Conti* und *Lockbit*. Die Vorgehensweise auch von anderen kriminellen Mitbewerbern ist gleich: Automatisiert werden Schwachstellen im IT-System von Unternehmen aufgespürt – und dann geschieht nach außen hin vorerst nichts. Intern aber wird Schritt für Schritt das System übernommen, die Organisation zu verstehen gelernt und es werden Firmendaten ausgespäht. Kommt es zum Impact, dass die Daten verschlüsselt werden und die Lösegeldforderung gestellt wird, wissen die Angreifer über die Finanzlage Bescheid, passen ihre Forderung dementsprechend an und kalkulieren, inwieweit sie allenfalls unter bestimmten Bedingungen noch Rabatt einräumen können. Wird Lösegeld bezahlt (womit man an sich eine kriminelle Organisation unterstützt), muss einkalkuliert werden, dass der übermittelte Schlüssel seinerseits

Fotos: Kurt Hickisch

Präsentation von innovativen Sicherheitsprodukten: Zutrittskontrollsystem, (Bargeld-)Wertbehältnis mit Einfärbungsfunktion

Fotos: Kurt Hickisch

ein Programm ist, das die Daten entschlüsselt. Der Zeitaufwand dafür geht über das Einspielen eines Backups hinaus und kann Wochen in Anspruch nehmen. Die beste Vorsorge besteht im Anlegen gesicherter Backups.

Wird kein Lösegeld bezahlt, werden die Datenpakete im Darknet verkauft. Ob bezahlt oder nicht, das betroffene Unternehmen scheint auf jeden Fall in einer Art Referenzliste auf, die eingesehen werden kann.

Ransomware wird auch als Service angeboten *(RaaS)* und kann gemietet werden, etwa, um Konkurrenten vom Markt zu drängen. Lösegeld wird auch verlangt, dass eine bei einem Unternehmen erkannte Schwachstelle nicht verraten wird *(Bug Bounty)*.

„Folgen Sie uns ins Internet, Ihre Daten sind schon lange dort", forderte der Vortragende des Netzwerks Cybercrime Komplettschutz, die Zuhörer zu einem Live-Einstieg ins Darknet auf der Website der Hacker-Gang *Lockbit* auf. Säuberlich aufgelistet fanden sich die zum Zeitpunkt des Aufrufs attackierten Unternehmen. Rot markiert waren dabei jene, bei denen der Countdown noch im Laufen war; grün hingegen jene, die der Lösegeldzahlung nicht nachgekommen und deren Daten zum Verkauf freigegeben sind. Als Folgen einer Ransomware-Attacke bezeichnete der Vortragende Datendiebstahl, Betriebsunterbrechung, Imageschaden, Haftpflichtansprüche, zivilrechtliche Sammelklagen und nach der DSGVO zu treffende Maßnahmen bzw. Folgen. Das auch als Aussteller im Foyer vertretene Unternehmen, ein Start-up, bietet neben IT-Leistungen und Fachvorträgen auch das Auslagern des Restrisikos einer Cyber-Attacke durch Versicherungslösungen an.

Datenregulierung. Dr. Gregor König, *Data Protection Officer* der *Erste Group,* stellte im Entwurf befindliche Gesetzesinitiativen der EU vor. War bisher der Schutz der Persönlichkeitsrechte (*privacy;* Beispiel DSGVO) im Vordergrund, ist nunmehr die Digitalisierung selbst Gegenstand der Regulierungsbestrebungen. Seit dem Referat bereits im Amtsblatt der EU veröffentlicht liegt der *Digital Markets Act* vor (Verordnung EU 2022/1925, in Kraft ab 1. November 2022), durch den große, systemische Online-Plattformen („Gatekeeper") unter anderem verpflichtet werden, gewerblichen Nutzern Zugriff auf die bei der Nutzung generierten Daten zu erlauben und den Plattformen andererseits verboten wird, eigene Produkte in der Reihung zu bevorzugen. Weitere Rechtsakte liegen im Entwurf vor, wie der *Artificial Intelligence Act,* durch den die künstliche Intelligenz geregelt werden soll. Durch den *Data Act* werden die Hersteller von IoT-Produkten verpflichtet, generierte Daten den Nutzern zur Verfügung zu stellen. Sehr große Online-Plattformen werden durch den *Digital Services Act* verpflichtet, mit den nationalen Behörden zusammenzuarbeiten. Die *European Digital Identity* soll einen EU-weiten elektronischen Identitätsnachweis ermöglichen und die *EU-IDAS*-Verordnung vertrauenswürdige elektronische Identitätslösungen EU-weit sicherstellen. Durch den *Digital Operations Resilience Act (DORA)* soll im Finanzsektor sowie im Bereich IKT-Dienstleistungen digitale Betriebsstabilität erreicht werden, um Cyber-Bedrohungen zu verhindern bzw. zu mindern. Die, insbesondere Telekommunikationsunternehmen betreffende *E-Privacy*-Verordnung, mit Regeln für Cookies und Marketing-Mails, hätte bereits 2018 in Kraft treten sollen, wird aber weiterhin politisch diskutiert.

Unter dem Titel „Der ganz normale Wahnsinn" stellte die Arbeitspsychologin Mag. Dr. Elisabeth Ponocny-Seliger Persönlichkeitstypen aus dem Arbeitsleben vor und zeigte auf, wie den entsprechenden Eigenheiten etwa des Kritischen, des Pessimisten, des Eigenwilligen, des Spontanen, des Ehrgeizigen, am besten begegnet werden kann.

Im Foyer waren Anbieter von Sicherheitsprodukten und -dienstleistungen mit Ausstellungsständen vertreten. Geräte zur Satelliten-Kommunikation stellte *Satellite Telecom (satellite-telecom.net)* vor, *Cennox (cennox.com)* Wertbehältnisse insbesondere für Bargeld. Eine Zerstörung dieser Behältnisse führt zum dauerhaften Einfärben von Banknoten. Das Unternehmen *safeREACH (safereach.com)* bietet Alarmierungslösungen an. Offline-Schließzylinder von *Datasec (datasec-electronic. com)* entsprechen dem herstellerübergreifenden Datenübertragungsstandard OSS, an dessen Entwicklung das Unternehmen maßgeblich beteiligt war und dem sich mittlerweile 83 Hersteller angeschlossen haben.

Das nächste Symposium Sicherheit wird am 10. und 11. Oktober 2023 stattfinden. *Kurt Hickisch*