Bild: beebright/stock.adobe.com

CYBERSECURITY CONFERENCE |

Achillesferse auf dem Silbertablett

Mit der fortschreitenden Digitalisierung wächst die Gefahr von Cyberattacken exponentiell. Viele Firmen sind darauf nicht vorbereitet. Wegen einer Gesetzesänderung können künftig auch Schwachstellen beim Datenschutz Unternehmen wirtschaftlich vernichten. In Mannheim zeigen Experten mögliche Auswege auf.

Ein Krieg tobt. Innerhalb von Sekundenbruchteilen wechseln die Angreifer, Ziele und Bündnisse. Rot, grün, gelb oder blau schießen Strahlen kreuz und quer über die Weltkarte, auf der sich die türkisumrandeten Nationen vom schwarzen Hintergrund abheben. Auf die Einschläge folgen Kreise. Rasch dehnen sie sich aus. Die „Norse Attack Map“, die an diesem Herbstmorgen in Echtzeit auf eine Leinwand im Mannheimer Rosengarten projiziert wird, ist nur eine von vielen Plattformen, die – wohl gemerkt nur die entdeckten – Hackerangriffe rund um den Globus veranschaulichen. Doch was aussieht wie ein futuristisches Science-Fiction-Spiel, repräsentiert ein in der Realität vorhandenes und im Zuge der Digitalisierung rasant wachsendes Problem. Dessen Folgen können Unternehmen wirtschaftlich schwer schädigen. Oder sogar vernichten.

„Cybersicherheit ist gerade für mittelständische Unternehmen eine Schicksalsfrage“, betont Josef Stumpf vom Bundesverband Mittelständische Wirtschaft (BVMW) Nordbaden-Rhein-Neckar. Er moderiert die zweite Auflage der Cybersecurity Conference in Mannheim. Zur Bündelung der IT-Security-Kompetenz in der Region wurde auf Initiative des IT-Beratungsunternehmens Sama Partners im vergangenen Jahr dieses Format ins Leben gerufen. Kooperationspartner sind die Stadt Mannheim, der BVMW, das Netzwerk Smart Production, der Bundesverband IT-Sicherheit TeleTrusT, die Information Systems Security Association (ISSA) und regionale Bildungseinrichtungen, etwa die Duale Hochschule Baden-Württemberg (DHBW) Mannheim, die Hochschule Mannheim und die Universität Mannheim.

In seiner Keynote verdeutlicht Dr. Dipl.-Ing. Ali Mabrouk, Geschäftsführer von Sama Partners, anhand eines ganz persönlichen Beispiels, welche Tragweite das Thema besitzt: „Meine Frau ist Ärztin, ich bin IT-Experte. Neulich haben wir unseren Sohn, der noch in die Grundschule geht, gefragt, was er später werden möchte.“ Seine Antwort: „Ich werde IT-Arzt.“ Für einige Sekunden geht ein Raunen durch den Raum, dann nicken immer mehr der über 100 Konferenzteilnehmer mit dem Kopf. „Würmer und Viren bergen auch für die IT eine enorme Gefahr“, fährt Mabrouk fort, „und damit für das gesamte Unternehmen.“

Statistiken belegen dies: Nach Angaben der EU-Kommission gab es 2016 weltweit 4000 Cyberangriffsversuche pro Tag – ein Anstieg um 300 Prozent im Vergleich zum Vorjahr. Den Schaden solcher Attacken schätzt die Kommission unter Berufung auf Europol allein in der EU auf 265 Milliarden Euro im Jahr. „Mit der fortschreitenden Digitalisierung geht ein exponentieller Anstieg der Cyberkriminalität einher“, warnt Gastgeber Mabrouk. Sie sei damit nicht nur „der Motor, der uns in die Zukunft katapultiert“, sondern zugleich eine „Achillesferse“ und ein „möglicher Grundstein für den Untergang“. Dessen Wucht und Reichweite vergleicht Mabrouk mit jener einer Atombombe. Dabei denkt er etwa an kritische Infrastrukturen wie Krankenhäuser oder Stromversorger.

Besonders schwer könnte diese Entwicklung den Mittelstand treffen, so der Experte. Viele kleine und mittlere Betriebe hätten die Bedrohung durch Cyberkriminelle bislang zu wenig ernst genommen. Das mache sie zu einer „leichten Beute“. IT-Sicherheit, das fordert auch Lars Göbel, Leiter Strategie & Innovation der DARZ GmbH, „muss eine deutlich höhere Priorität bekommen“. Er zeigt das an einem Beispiel aus der Praxis: Ein Virus verschlüsselte die Daten in der Geschäftssoftware eines mittelständischen Betriebs. „Für eine Woche stand alles still“, sagt Göbel. „So etwas dürfte es eigentlich nicht mehr geben.“

Ali Mabrouk kommt der Fall eines Unternehmens mit Tochterfirmen in Österreich und der Schweiz in den Sinn. Über Monate verschwieg der Verantwortliche in der Schweiz einen erfolgreichen Angriff. Daraufhin infizierte der Virus auch den Mutterkonzern. „Es entstand ein Millionenschaden“, unterstreicht der IT-Sicherheitsspezialist. In welcher Größenordnung Daten verlorengingen, sei bis heute unklar. Vor diesem Hintergrund fordert Mabrouk eine stärkere „Cyberhygiene“ in Unternehmen. Mitarbeiter benötigen demnach ein gesteigertes Bewusstsein für Gefahren aus dem Netz – und klare Regeln für den Umgang mit der IT.

Chef als Sicherheitslücke?

Doch gerade in den oberen Hierarchieebenen lauern Risiken: „Wenn der Chef aus dem Urlaub E-Mails von seinem Freemail- oder GMX-Account schickt, war vielleicht alles umsonst“, weiß Stefan Becker aus Erfahrung. Er leitet das Referat „Cybersicherheit in der Wirtschaft“ beim Bundesamt für Sicherheit in der Informationstechnik (BSI). „Wer Cyberkriminalität erfolgreich bekämpfen will, muss angemessenes Verhalten auch top-down vorleben“, konstatiert Becker.

In seinem Vortrag warnt er zudem vor dem sogenannten CEO Fraud. Bei dieser Betrugsmasche verschicken Kriminelle vermeintlich von der Geschäftsführung ausgehende E-Mails, in denen sie die Überweisung meist beträchtlicher Summen anordnen. „Im Zweifelsfall sollten Mitarbeiter das Telefon als zweiten Kommunikationsweg zur Verifizierung nutzen“, sagt Becker. Aber auch dies biete keinen 100-prozentigen Schutz. Hierzu ruft er sich sowie den Zuhörern einen konkreten Fall in Erinnerung: Betrüger, die es auf ein Finanzunternehmen abgesehen hatten, fälschten demnach nicht nur Dokumente und Unterschriften täuschend echt. Selbst den professionellen Rückfragen in einem – freilich umgeleiteten – Telefonat hielten die Drahtzieher überzeugend stand. ▸▸

Doch nicht nur der fehlende Schutz vor Cyberattacken kann verheerende Konsequenzen haben. Für den Datenschutz gilt das ebenfalls. Schon das seit Juli 2015 geltende IT-Sicherheitsgesetz stellt die Unternehmen vor eine Reihe von Schwierigkeiten, wie Stephan Krätzschmar, Senior Security Consultant bei Sama Partners, darlegt. So gebe es darin eine Reihe von unspezifischen Begriffsdefinitionen, zum Beispiel „Stand der Technik". Allein hierzu habe der Bundesverband IT-Sicherheit TeleTrusT eine 64 Seiten umfassende Handreichung herausgegeben. Zudem mache es der „Allgefahrengrundsatz" nötig, alle möglichen Risiken zu berücksichtigen und zu bewerten. Auch sei die Betreiberfrage nicht eindeutig geklärt. Daher können Unternehmen sich Krätzschmar zufolge „nicht einfach zurücklehnen und die Verantwortung etwa an einen Dienstleister mit Rechenzentrum outsourcen".

Verschärft werden die Herausforderungen durch die 2016 in Kraft getretene EU-Datenschutz-Grundverordnung (DSGVO), die ab dem 25. Mai 2018 greift. Im Gegensatz zur Richtlinie 95/46/EG muss sie nicht erst in nationales Recht umgesetzt werden. Sie gilt unmittelbar. „Erklärtes Ziel ist es, die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit zu vereinheitlichen", erläutert Krätzschmar. Zu diesem Zweck sei etwa das „Marktortprinzip" etabliert worden: Die DSGVO betrifft somit alle Unternehmen, die im europäischen Markt agieren – ungeachtet dessen, ob sie innerhalb der EU mit einem Firmensitz vertreten sind. Vor allem US-amerikanische Konzerne versuchen laut Krätzschmar, „mit aller Lobbykraft dagegen vorzugehen". Das Recht auf „Vergessenwerden" sowie zur Datenmitnahme dürften ebenfalls europäischen Unternehmen zu schaffen machen. Wie Stephan Krätzschmar ausführt, ergeben sich daraus Probleme bei der Datenübertragung etwa bei einem Bank-, Versicherungs oder Energieversorgerwechsel.

„Cybersicherheit ist gerade für mittelständische Unternehmen eine Schicksalsfrage."

Josef Stumpf,
Leiter der Geschäftsstelle des BVMW-Kreisverbands Nordbaden-Rhein-Neckar

Auf zwei besonders gravierende Änderungen weist Dr. Stefan Brink, Landesbeauftragter Datenschutz Baden-Württemberg, hin. Eine davon betrifft die Umkehr der Beweislast: Behörden müssen künftig nicht mehr Verstöße nachweisen. Stattdessen müssen Unternehmen verdachtsunabhängig dokumentieren, dass sie die geltenden Regeln einhalten. „In Zukunft wird es wirtschaftlich vernünftig sein, sich um Datenschutzfragen zu kümmern", ist der frühere Richter überzeugt. Das gelte insbesondere mit Blick auf die Geldbußen, die „unverhältnismäßig und brutal" erhöht worden seien. „Sie sollen abschrecken." Brink rechnet vor: Ging es bisher maximal um einige Hunderttausend Euro, werden künftig, abhängig von der Schwere des Verstoßes, bis zu zehn Millionen Euro (Artikel 25 / geregelt in Artikel 83 Absatz 4a) oder gar 20 Millionen Euro (Artikel 5 / geregelt in Artikel 83 Absatz 5a) fällig. Oder noch schlimmer: Ergeben zwei Prozent (Artikel 25) respektive vier Prozent (Artikel 5) des vorherigen Jahresumsatzes der Firmengruppe einen höheren Betrag, muss diese Summe als Strafe gezahlt werden. „Einmal übersteht das ein Unternehmen vielleicht", schätzt Brink, „ein zweites Mal höchstwahrscheinlich nicht."

Beratung im konkreten Fall

Konkret veranschaulicht der Landesdatenschutzbeauftragte das an einem Beispiel aus der Vergangenheit. Die Bahn hatte über Jahre hinweg heimlich die Daten ihrer Mitarbeiter mittels eines sogenannten Screenings mit denen von Lieferanten verglichen, um Korruptionsfälle aufzudecken. Außerdem ließ sie in Verdachtsfällen durch Detektive Konto- und andere sensible Daten sammeln, auch solche von Angehörigen der Beschäftigten. Das verstieß gegen geltendes Recht und kostete den Konzern gut 1,1 Millionen Euro Bußgeld sowie Hartmut Mehdorn seinen Posten als Vorstandsvorsitzender. „Mit der neuen Regelung könnte in einem vergleichbaren Fall statt einer Million eine Milliarde Euro fällig werden", warnt Brink. Eine strikt vom für die Bußgelder zuständigen Bereich getrennte Abteilung der Landesbehörde berate Unternehmen darin, im individuellen Fall die gesetzlichen Vorgaben korrekt umzusetzen. „Der Berater mit dem sprichwörtlichen Holzhammer in der Hosentasche klingt ein bisschen nach Widerspruch", räumt Brink ein. Es gehe jedoch darum, frühzeitig zu agieren und mögliche Konflikte konstruktiv zu lösen, bevor eine Strafe drohe. Angesichts der zunehmenden Belastung werde die Behörde personell deutlich wachsen.

„Einmal übersteht das ein Unternehmen vielleicht, ein zweites Mal höchstwahrscheinlich nicht."

Dr. Stefan Brink,
Landesbeauftragter Datenschutz Baden-Württemberg, vor dem Hintergrund drastisch steigender Bußgelder, die im Zuge der EU-Datenschutz-Grundverordnung ab Mai 2018 bei Verstößen drohen

Zwar sind die bisherigen Gesetze auf nationaler Ebene nicht aufgehoben, doch das EU-Recht besitzt Geltungsvorrang. Dementsprechend ist die oberste juristische Instanz der Europäische Gerichtshof (EuGH). „Das Bundesverfassungsgericht wird nichts mehr zu entscheiden haben", so Brink. Zugleich erhofft er sich von der DSGVO klarere Strukturen und einen Zuwachs an Rechtssicherheit für die Unternehmen im Land. „Bis zur Verabschiedung war es ein langer und schwieriger Weg", sagt Brink. „Dass jemand innerhalb der nächsten zehn Jahre die neuen Regelungen antasten wird, ist sehr unwahrscheinlich."

Im weiteren Verlauf der Konferenz referieren noch Prof. Dr. Sachar Paulus von der Hochschule Mannheim zum Thema „Security by Continuous Delivery" und Dario Engelmayer, Security Consultant bei Sama Partners, zu „VPN – Schwachstellen und Schutzmaßnahmen". Ronny Kaminski, Senior Consultant und Mitglied der TeleTrusT Arbeitsgruppe „Mobile Security", sensibilisiert das Publikum zu den besonderen Gefahren der geschäftlichen Nutzung von Smartphone und Tablet – von infizierten Apps über SMS-Phishing bis hin zu Social Engineering.

Ob mobil oder am Rechner: Cybersicherheit muss Chefsache sein. Darin sind sich die Teilnehmer der abschließenden Diskussion einig. Gleichzeitig, sagt Stefan Becker vom BSI, sollten Entscheider versuchen, alle Mitarbeiter mitzunehmen und sie von den Vorteilen des Konzepts zu überzeugen – selbst wenn dieses mehr Aufwand bedeute. „Einen sicheren Hafen", das macht Prof. Dr. Sachar Paulus unmissverständlich klar, „gibt es nicht mehr." Umso wichtiger ist es für Unternehmen, sich rasch für die bevorstehenden Angriffe aus dem Netz zu wappnen. Der Krieg tobt längst. *Dennis Christmann*