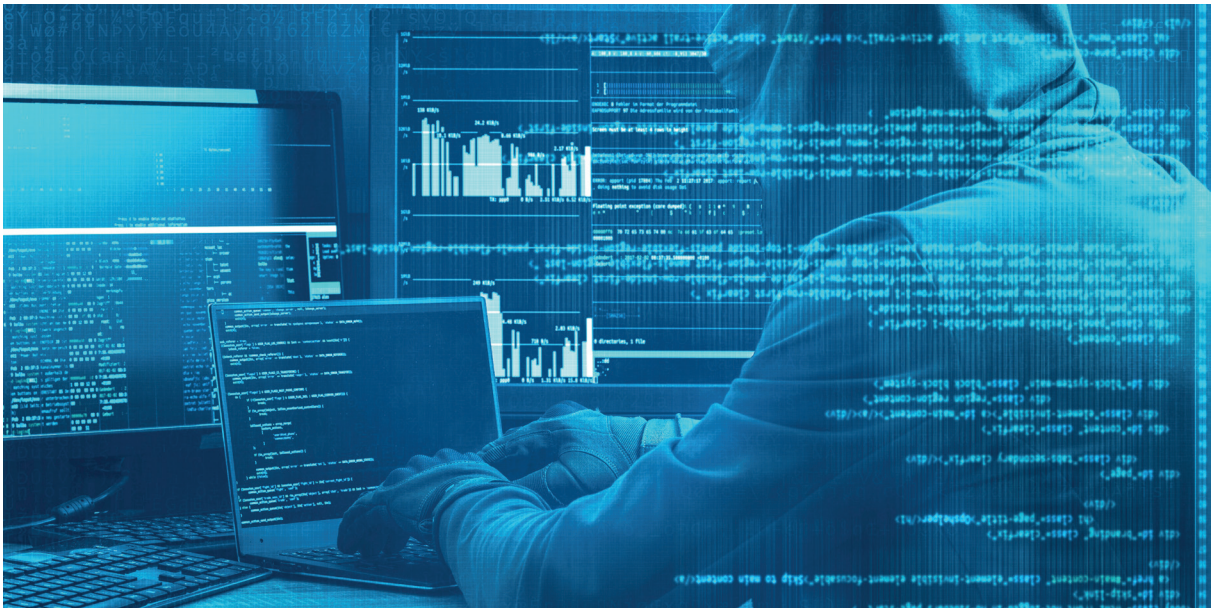
WWW.OEAW.AC.AT

ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN



FORSCHUNG UND GESELLSCHAFT | 18

BLACKOUT DURCH CYBERWAR

FIKTION ODER REALITÄT?

BLACKOUT DURCH CYBERWAR

FIKTION ODER REALITÄT?

PODIUMSDISKUSSION
AM 16. SEPTEMBER 2019

ÖAW

INHALT

EDITORIAL

GEORG BRASSEUR

„Einen Augenblick lang verstummt alles. Dann treten die Folgen eines Stromausfalls abrupt und massiv auf. Im ganzen Land fallen auf einen Schlag die Ampeln aus. Tausende Unfälle ereignen sich gleichzeitig. Unzählige Menschen stecken in Zügen, U-Bahnen und Fahrstühlen fest.

Aus: „Quarks & Co bei Planet Schule, Strom – Die Revolution im deutschen Netz", 27.06.2012; WDR

Ist ein landesweiter Stromausfall, also ein Blackout, Fiktion oder Realität? Fest steht: Ein Szenario wie dieses zeigt die Verwundbarkeit unserer modernen Welt, in der ohne elektrische Energie so gut wie gar nichts mehr funktioniert. Ein tagelang andauernder, landesweiter Stromausfall kann, wie Beispiele aus der Vergangenheit zeigen, schwerwiegende Folgen für die Wirtschaft und die Gesellschaft haben. Die Stromversorgung ist daher DIE kritische Infrastruktur jedes hoch industrialisierten Landes. Längst gehören Cyberangriffe zur erklärten Maßnahme, ein Land gezielt zu destabilisieren und einen Zusammenbruch herbeizuführen. Die wachsende Vernetzung von Computersystemen, der enorme Digitalisierungsschub und die Fortschritte bei der Entwicklung künstlicher Intelligenz erhöhen zudem die Möglichkeiten von Attacken auf der Software-Ebene. Ein sogenannter Cyberwar entbrennt zwischen Konfliktparteien, wird anfänglich im Stillen geführt und greift die Souveränität eines Landes an.

Ob die Lahmlegung der Stromversorgung durch Aktionen im Rahmen eines Cyberwars eine reale Bedrohung darstellt, oder – vom Stand der Technik betrachtet – nur Fiktion ist, war die zentrale Frage der von der ÖAW initiierten Podiumsdiskussion, bei der Expertinnen und Experten wissenschaftsbasiert über Cyberattacken und Cyberabwehr, über Energienetze und völkerrechtliche Aspekte diskutierten.

In der vorliegenden Publikation können Sie den Verlauf der Debatte nachvollziehen und erhalten im Schlusswort eine zusammenfassende Deutung des Gesagten. Die ÖAW bietet mit dieser Publikation einer breiten Öffentlichkeit die Grundlagen und eine faktenbasierte Orientierung zu einem alle Lebensbereiche betreffenden Thema.

BEGRÜSSUNG UND EINLEITUNG

GEORG BRASSEUR

Meine sehr geehrten Damen und Herren, liebe Kolleginnen und Kollegen, im Namen des Präsidiums der Österreichischen Akademie der Wissenschaften heiße ich Sie im Festsaal der Akademie herzlich willkommen. Während Sie im Saal Platz genommen haben, lief ein fünf Minuten langes Video, das einige Hard Facts zum Thema Cyberattacken aufgezeigt hat: Beispielsweise dass weltweit pro Sekunde 12 mit dem Internet verbundene Personen von Cyberattacken betroffenen sind, dass fast die Hälfte der Kriminalität in England „Cybercrime" zuzuschreiben ist, dass in den USA der Diebstahl von personenbezogenen Daten die am schnellsten wachsende kriminelle Handlung darstellt, dass täglich mehr als 230.000 neue Schadsoftware-Programme im Internet auftauchen und dass im Jahr 2018 Konsumentinnen und Konsumenten weltweit 158 Milliarden US-Dollar durch Cybercrime verloren haben.[1] Was ist davon Fiktion? Was ist Realität? Zu diesen Fakten werden wir später in der Diskussion zurückkehren. Doch zunächst begrüße ich insbesondere hochrangige Vertreterinnen und Vertreter der Parlamentsdirektion, des Bundesministeriums für Landesverteidigung und des Außenministeriums sowie Personen aus einem Unternehmen der Privatwirtschaft im Energie-, Computer- und Sicherheitssektor, da wir uns heute dem Thema „elektrische Energie" widmen. Natürlich

Georg Brasseur, Professor für Elektrische Meßtechnik und Meßsignalverarbeitung an der Technischen Universität Graz, wurde 2012 zum wirklichen Mitglied der ÖAW gewählt. Seit 2013 ist er Präsident der mathematisch-naturwissenschaftlichen Klasse.

[1] *Hackerpocalypse: A Cybercrime Revelation*, Steve Morgan, Editor-in-Chief, Cybersecurity Ventures; A 2016 Report from Cybersecurity Ventures sponsored by Herjavec Group, Q3 2016; p. 6
http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

begrüße ich auch die Mitglieder der Österreichischen Akademie der Wissenschaften, unsere Mitarbeiterinnen und Mitarbeiter sowie Medienvertreterinnen und Medienvertreter. Mein besonderer Gruß und Dank richtet sich an die vier Podiumsgäste: Carina Kloibhofer, Walter Unger, Dietmar Mandl und August Reinisch. Sie werden später vom Moderator näher vorgestellt werden. Und last but not least begrüße ich unseren Moderator, Thomas Eiter, der Sie durch die Veranstaltung begleiten wird.

Die Österreichische Akademie der Wissenschaften hat den gesetzlichen Auftrag, die Wissenschaft in jeder Hinsicht zu fördern. 1847 als Gelehrtengesellschaft gegründet, hat sie gegenwärtig mehr als 760 Mitglieder und rund 1.800 Mitarbeiterinnen und Mitarbeiter, die sich der innovativen Grundlagenforschung, dem interdisziplinären Wissensaustausch und der Wissensvermittlung widmen. Die große Anzahl der Mitarbeiterinnen und Mitarbeiter ist auch darauf zurückzuführen, dass die Akademie zahlreiche Forschungsinstitute auf höchstem wissenschaftlichen Niveau betreibt. Die Mitglieder bilden die Gelehrtengesellschaft und stellen sich einem regen fachübergreifenden Austausch in wichtigen Zukunftsfragen. Sie informieren Politik und Gesellschaft über neue wissenschaftliche Erkenntnisse. Die Akademie ist ein lebendiger Ort, an dem wissenschaftliche Leistungen und Erkenntnisse vermittelt werden. Sie bietet intellektuellen Raum für Diskussion, fördert eine Gesellschaft, die offen für Wissenschaft und Technologie ist, und versucht, das Bewusstsein für aktuelle wissenschaftliche und gesellschaftliche Herausforderungen zu schärfen.

Die verschiedenen Veranstaltungen, die sich insbesondere auch an junge Menschen richten, sollen frühzeitig die Faszination für Wissenschaft, Forschung und Technologie wecken. Der Film, den Sie schon am Anfang gesehen haben, sollte Sie auf das einstimmen, was jetzt kommen wird – nämlich ein Bedrohungsszenarium. Ein Bedrohungsszenarium, das mit Datendiebstahl beginnen kann, Stichwort Hackerangriffe, und bis zum Angriff auf die Souveränität eines Landes gehen kann und damit als Cyberwar bezeichnet wird. Heute steht das Thema elektrische Energie im Vordergrund, daher auch der Titel: Blackout durch Cyberwar.

Damit übergebe ich das Mikrofon an Thomas Eiter, Professor für Wissensbasierte Systeme am Institut für Informationssysteme der Technischen Universität Wien und seit 2007 korrespondierendes Mitglied der Österreichischen Akademie der Wissenschaften.

PODIUMS-DISKUSSION

Thomas Eiter, Professor für Wissensbasierte Systeme an der TU Wien, Institut für Logic and Computation, ist seit 2007 korrespondierendes Mitglied der mathematisch-naturwissenschaftlichen Klasse im Inland.

THOMAS EITER

Vielen Dank. Im eingangs gezeigten Film stand Cyberkriminalität als Bedrohung im Vordergrund. Wir werden uns heute auf kritische Infrastruktur konzentrieren, speziell auf den Energiesektor. Sonst könnten wir dieses Thema gar nicht erschöpfend behandeln. Es freut uns, dass wir dafür vier Expertinnen und Experten gewonnen haben und ich bitte Carina Kloibhofer, Research Engineer am Austrian Institute of Technology (AIT), auf das Podium. Ich ersuche Sie, uns zu erzählen, was Sie beruflich machen, und bitte klären Sie uns auch über einige der im Film genannten Begriffe auf. Zum Beispiel war von Ransomware die Rede, was versteht man darunter?

CARINA KLOIBHOFER

Als Research Engineer am Austrian Institute of Technology beschäftige ich mich mit interdisziplinärer Sicherheitsforschung in den unterschiedlichsten Domänen. Darüber hinaus, weil Sicherheitsforschung immer am aktuellen Stand sein muss, befasse ich mich auch mit der Implementierung von technischen und organisatorischen Maßnahmen gegen die täglichen Bedrohungen in den unterschiedlichsten Domänen. Was sind nun typische tägliche Bedrohungen? Sie haben es gerade angesprochen: zum Beispiel Ransomware. Ransomware ist vor allem eine Attacke auf die Verfügbarkeit der Daten. Zum Beispiel die Ransomware „Cryptolocker“, eine Ausprägung, wo Daten tatsächlich auch verschlüsselt werden und damit nicht mehr zugreifbar sind. Das zielt in der Regel auf Erpressung ab. Das heißt, hier stehen meist monetäre Ziele der An-

Carina Kloibhofer, MSc MSc, Research Engineer am Center for Digital Safety & Security, Austrian Institute of Technology GmbH (AIT).

greifenden dahinter. Darüber hinaus kam im Film auch der Begriff DDoS vor, also „Distributed-Denial-of-Service"-Attacken, die ebenfalls auf die Verfügbarkeit von Daten abzielen. Unter Zuhilfenahme der Rechenpower einer großen Anzahl unterschiedlicher Rechner wird eine Überlastung der IT-Infrastruktur herbeigeführt. Auch hier liegt der Fokus darauf, die Verfügbarkeit der Daten zu blockieren, um dann die Lösung in Form eines externen Services gegen Geld anzubieten oder um ungesehen in Datennetzwerke einzudringen und illegale Transaktionen zu tätigen.

THOMAS EITER

Wir werden sicher noch Gelegenheit haben, mehr darüber zu sprechen, insbesondere auch in Bezug auf das heutige Thema. Der nächste Teilnehmer am Podium ist Dietmar Mandl, Chief Information Security Officer und Datenschutzbeauftragter der Austrian Power Grid AG (APG). Für die heutige Veranstaltung vertritt er die Rolle des Angegriffenen. Vielleicht können Sie uns ein bisschen über Ihre Tätigkeit erzählen.

DIETMAR MANDL

Die Austrian Power Grid AG betreibt das Höchstspannungsnetz in Österreich und gewährleistet die sichere Stromversorgung Österreichs. Als unabhängiger Übertragungsnetzbetreiber Österreichs ist die Kernaufgabe der APG, diese Balance in jedem Moment zu halten. Die Stromversorgung funktioniert nach einem wesentlichen Prinzip: Stromerzeugung und Stromverbrauch müssen sich in jeder Sekunde exakt die Waage halten. Nur dann ist das System stabil und die Versorgung sichergestellt. Als Chief Information Security Officer habe ich ein sehr umfassendes und breites Aufgabengebiet inne. Eine der wichtigsten Tätigkeiten ist sicherlich das Risikomanagement. Neben der durchdringenden Vernetzung und dadurch Erhöhung der Komplexität des Gesamtsystems ändert sich auch zunehmend die Bedrohungslage. Daher müssen laufend die Bedrohungsszenarien analysiert und ein möglicher Schaden für das Unternehmen mit der entsprechenden Eintrittswahrscheinlichkeit bewertet werden. Da uns nicht unlimitierte Ressourcen zur Verfügung stehen, werden im Anschluss Maßnahmen risikobasiert abgeleitet.

THOMAS EITER

Nachdem wir von Angriff und dem Objekt der Begierde gehört haben, wäre dann die Verteidigung das nächste Thema. Ich darf dazu Walter Unger, Oberst des Generalstabsdienstes und Leiter der Cyber-Defence-Abteilung des Abwehramtes, angesiedelt im Bundesministerium für Landesverteidigung, auf das Podium bitten.

WALTER UNGER

Der Begriff Security gehört dem Innenressort. Wir sind die, die das Land verteidigen, auch im Cyberraum. 2003 gab es die Bundesheerreformkommission unter dem Vorsitz des ehemaligen Bürgermeisters Helmut Zilk, da habe ich zwischen Tür und Angel von einem General den Auftrag bekommen: „Und du beschäftigst dich jetzt mit Cyberwar und Cyberterrorismus und dem Schutz kritischer Infrastrukturen."
Aus dieser kurzweiligen Beschäftigung ist eine 150 Seiten starke Studie entstanden. Die hat einen großen, roten Stempel oben drauf. Was so viel bedeutet wie: geheim. Das hat einen großen Vorteil und einen großen Nachteil. Der Nachteil ist, der Geheimstempel sorgt dafür, dass das möglichst wenige Leute lesen. Aus diesem Grund – bis 2008 fast unbekannt – durfte ich dann das erste Mal in der Gesellschaft für Politisch-Strategische Studien an der Landesverteidigungsakademie dazu vortragen. Und da hatte ich beim Blick ins Publikum das Gefühl, die Leute glauben, der ist doch jetzt vom Mars gefallen. Ich habe Cyberwar-Szenarien dargestellt, was alles passieren kann. Bei einigen im Publikum dachte ich, die glauben, ich bin jetzt direkt aus Hollywood angereist. Zwei Jahre später haben wir den Stuxnet (*Computerwurm-Cyberattacke auf Industrieanlagen des Iran 2010, Red.*) erlebt. Und das war dann wirklich ein Wake-up-Call. Österreich hat sich aus der damals noch dahinplätschernden Diskussion heraus sehr ernsthaft mit der Thematik beschäftigt und 2013 die Cyber-Security-Strategie Version 1 beschlossen, nach der dann über Jahre jetzt einige Instrumente aufgebaut wurden, die uns vor solchen Gefahren schützen sollen. Parallel dazu ist meine 2001 aufgestellte Abteilung fünf Mal vergrößert worden. Einfach deshalb, weil unser Militär erkannt hat, dass wir von

Dietmar Mandl, MSc, Chief Information Security Officer and Data Protection Officer der Austrian Power Grid AG (APG).

Oberst Walter Unger, Leiter der Abteilung „Cyber Defence", Abwehramt des österreichischen Bundesheeres, Bundesministerium für Landesverteidigung (BMLV).

diesen IT-Infrastrukturen abhängig sind. Wir müssen sie entsprechend schützen. Und dieser Schutz endet natürlich nicht am Kasernentor. Dann hätte das Militär seinen Hauptzweck nicht erfüllt, sondern wir müssen natürlich nachdenken, was bedeutet Landesverteidigung im Cyberraum. Was bedeutet es, einen virtuellen Raum zu verteidigen?

THOMAS EITER

Nach diesem umfassenden Einblick in die Entwicklung der Cyber-Defence-Abteilung bitte ich als letzten im Quartett August Reinisch von der Universität Wien, Institut für Europarecht, Internationales Recht und Rechtsvergleichung auf das Podium. Das Ganze hat ja auch eine rechtliche Dimension beziehungsweise ist es eine rechtlich sehr spannende Frage, wie diese Art von Angriffen, Cyberattacken zu bewerten sind. Wie geht man damit um? Aus strafrechtlicher Sicht und auch aus völkerrechtlicher Sicht? Ist das Neuland? Wir kommen gleich zu Ihren Antworten. Doch zunächst: Unser Thema heute ist die Energie. Kritische Energieinfrastruktur, insbesondere also Strom. Nur um einmal ein Gefühl dafür zu bekommen, wie stark wir vom Strom abhängig sind, haben wir einen Film vorbereitet, der vom Westdeutschen Rundfunk, dem WDR, erstellt worden ist[2] und der uns vor Augen führt, welche Ausmaße ein Blackout, der länger anhält, erreichen kann.

> *Während die Situation in den Städten eskaliert, tickt vor den Städten eine Zeitbombe. Atomkraftwerke brauchen Kühlung. Bricht hier die Notstromversorgung zusammen, droht die Kernschmelze. Eine Woche ohne Strom würde unsere Gesellschaft nicht überstehen.*
> *(Zitat: Schlusskommentar aus dem gezeigten Film)*

THOMAS EITER

Das war doch ein sehr ernüchternder Film, der uns unsere Abhängigkeit von Strom sehr klar vor Augen führt. Frau Kloibhofer, ich möchte mit Ihnen beginnen und nochmals die Frage stellen: Ist dieses Szenario realistisch? Könnte man einen An-

[2] Quarks & Co bei Planet Schule, Strom – Die Revolution im deutschen Netz, 27.06.2012.

griff in dieser Dimension gestalten, um so einen Blackout zu bewirken?

CARINA KLOIBHOFER

Über die Auswirkungen wissen die Kolleginnen und Kollegen wahrscheinlich mehr. Aber so ein Angriff an sich ist natürlich vorstellbar. Jede Institution, jede kritische Infrastruktur oder die Betreiber wesentlicher Dienste, wie sie jetzt heißen, sind natürlich angreifbar. Es gibt kein System, das zu 100 Prozent sicher ist, und es gibt immer auch Lücken, die man finden kann. Es stellt sich immer nur eine Frage: Wie viel ist der Angreifer bzw. die Angreiferin bereit zu investieren? Und die Gegenfrage ist: Wie viel ist die Organisation oder ist der Staat bereit zu investieren, um sich abzusichern?

THOMAS EITER

Also ist es letztendlich eine Kostenfrage? Wenn man die entsprechenden Mittel aufwendet, könnte man das Problem vermeiden und absolute Sicherheit erzielen?

CARINA KLOIBHOFER

Absolute Sicherheit ist meiner Meinung nach nie erreichbar. Es gibt keine hundertprozentige Sicherheit. Aber natürlich, je mehr ich bereit bin, seien es jetzt Kosten, monetäre Mittel oder andere Ressourcen zu investieren, umso höher ist der Grad der Absicherung, den ich erreichen kann.

DIETMAR MANDL

Ich möchte die Aussage unterstreichen: Hundertprozentige Sicherheit gibt es nicht. Wir sind alle, wie man es im Film auch sehr schön gesehen hat, abhängig von elektrischem Strom. Alle gehen davon aus, dass sie, wenn der Ladestand des Handy-Akkus leer ist, zur Steckdose gehen und diesen ohne Probleme aufladen können. Genauso wie das Internet für uns alle mittlerweile schon selbstverständlich ist. Beim Strom haben wir zusätzlich dieses Thema, dass die ganze Gesellschaft von diesem Lebenselixier abhängt. Darüber hinaus haben wir in Zentraleuropa, und auch speziell in Österreich, eine hohe Güte der Versorgungssicherheit. Große oder länger andauernde Stromausfälle bewegen sich im Bereich von einer halben Stunde bis Stunde, maximal ein paar Stunden. In Ländern mit einer schlechteren Versorgungsqualität treten lokale Stromausfälle wesentlich häufiger auf. Daher sind die Menschen dort besser auf länger andauernde Unterbrechungen der Stromversorgung vorbereitet. Der letzte große Stromausfall in Südamerika ist ein Szenario, welches natürlich auch auf Österreich zutreffen könnte, wenngleich ich die Eintrittswahrscheinlichkeit als gering ansehe. Es sollte sich daher jede und jeder bewusst sein, dass so etwas passieren kann und sich in gewissem Maße darauf vorbereiten. Die APG trifft selbstverständlich umfassende Vorkehrungen, dass so etwas nicht eintritt, hundertprozentig ausschließen kann man es jedoch nicht.

THOMAS EITER

Und wie ist unsere Energiewirtschaft aus Ihrer Sicht gewappnet?

DIETMAR MANDL

Die Energiewirtschaft ist meines Erachtens sehr gut organisiert. Es wird ein regelmäßiger Austausch unter-

einander gepflegt und es werden laufend Übungen durchgeführt. Es werden auch gemeinsam mit Behörden und Einsatzorganisationen Übungen durchgeführt, um Katastropheneinsätze begleiten und durchexerzieren zu können. Leider ist es nicht so einfach möglich, den Strom auszuschalten und den Ernstfall durchzutesten. Das ist die große Kunst dabei, das vorab soweit antizipieren zu können und dann in einem Planspiel durchzugehen. Grundsätzlich denke ich, dass die österreichische und auch die europäische Energiewirtschaft sehr gut abgestimmt sind. Das ist auch notwendig, weil das Energiesystem heutzutage wesentlich komplexer ist als früher. Durch die Dekarbonisierung, den Ausstieg aus fossiler Energie, und den Atomausstieg werden konventionelle Kraftwerke sukzessive durch erneuerbare Energien wie Wind und Sonne ersetzt. Leider lässt sich überschüssige Wind- und Sonnenenergie nicht so einfach speichern. Das ist zusätzlich ein komplexes Thema, das jetzt vielleicht gar nichts mit Cyber-Security zu tun hat, aber das Gesamtsystem einfach immer komplexer werden lässt.

THOMAS EITER

Sie haben die Zusammenarbeit mit Behörden erwähnt. Diese Bedrohungsszenarien, die wir gesehen haben, können ja durchaus einen vielfältigen Hintergrund haben. Auf jeden Fall würde man aber an die Cyber-Defence-Abteilung als erste Behörde denken. Könnte man aus Ihrer Sicht solche Angriffe abwehren? Was kann man dagegen unternehmen?

WALTER UNGER

Das vorhin gezeigte Szenario ist in etwa das, was wir angenommen haben, bevor wir überlegt haben: Was tun wir denn jetzt eigentlich? Wir haben eine These formuliert, die lautet: Jeder Staat ist von seinen wichtigen Infrastrukturen, von seinen strategisch bedeutsamen und – wenn sie ausfallen – daher kritischen Infrastrukturen abhängig. Diese Infrastrukturen sind heute weitestgehend davon abhängig, dass dahinterstehende Netzwerke, IT-basierte Netzwerke, Computer funktionieren. Daher wäre es eine Überlegung für einen Aggressor, man attackiert über die Netze diese Infrastrukturen und erzwingt so politische Zugeständnisse. Das heißt, man rückt nicht mit Soldaten aus, man kommt nicht mit Fliegern, man kommt mit Cyberangriffen. Das war die These und diese haben wir überprüft. Wie wir vorher schon gehört und hier gesehen haben, sind wir also weitestgehend von diesen Infrastrukturen abhängig. Wir haben eine sehr arbeitsteilige Infrastruktur aufgebaut, Just-in-Time und so weiter. Alle kritischen Infrastrukturen sind von funktionierenden Computern abhängig, beginnend von der Stromversorgung und der Telekommunikation, den Notfalldiensten und den Behörden, die besonders wichtig sind in solchen Situationen, über die Luftraumüberwachung und logistischen Systemen bis hin zum Wasser und zur Abwasserentsorgung. Das ist einem im Alltagsleben nicht bewusst. Damit müssen wir jetzt leben. Wir müssen damit rechnen, es könnte Leute geben, die wollen von Österreich politisch etwas und überlegen sich, wie kann man Österreich möglichst ohne Waffengewalt, sondern nur mit Cyberangriffen in die Knie zwingen. Und ich fürchte, das ist denkbar. Und daher ist es auch eine logische Entwicklung in Österreich, dass wir 2013 die Cyber-Security-Strategie

entwickelt und fertiggestellt haben. Gar nicht viel später als die meisten Länder. Einige Länder waren noch später dran. Seitdem haben wir Infrastrukturen. Dabei wurde zunächst einmal die Frage geklärt, wer eigentlich zuständig ist in Österreich.
Das ist aus meiner Sicht relativ eindeutig. Wir werden es dann noch genauer hören. So lange Frieden ist, bis hin zur Krisensituation, ist das Innenministerium zuständig. Und erst wenn ein Verteidigungsfall ausgerufen wird, ist das Militär zuständig. Welche Ausnahmesituationen auch immer in Friedenszeiten auftreten, das Militär ist unsere einzige strategische Reserve hier in Österreich. Egal ob irgendwo zu viel Schnee fällt oder es zu viel regnet oder ob an der Grenze die Polizei Unterstützung braucht, kann das Militär zur Assistenz, zur Amtshilfe herangezogen werden. Und das ist natürlich auch im Cyberbereich vorstellbar. Entsprechend wurden auch die operativen Elemente – dazu kommen wir noch – in Österreich aufgestellt, nämlich in enger Kooperation zwischen dem Innenressort und unserem Ressort.

THOMAS EITER

Sie haben von Cyberattacken gesprochen und der Frage, wer hinter diesen Attacken steht. Sie haben erwähnt, dass dies jemand sei, der etwas von einem Staat beziehungsweise der Regierung will. Können das nur Kriminelle sein? Können das Terroristen sein? Oder können auch Staaten dahinterstehen? Und welche Möglichkeiten hätte man, das überhaupt festzustellen?

WALTER UNGER

Man muss sich natürlich fragen: Welche Motive verfolgt der Angreifer oder die Angreiferin? Und daraus kann man dann Rückschlüsse ziehen, woher die Aktion kommt. Weil diese Frage, die Attribution, nämlich die Zuordenbarkeit, wer steckt dahinter, ist keineswegs endgültig oder gar technisch schon gelöst. Es gibt Annäherungen dazu. Man erkennt das daran, dass man seit einem Jahr auch die Beteiligten benennt. Wenn man früher gelesen hat, das könnte der oder der gewesen sein, liest man heute, die chinesische Gruppierung, die nordkoreanische, die russische oder eine andere Gruppierung steckt dahinter. Das heißt, Großmächte im Cyberbereich haben Methoden entwickelt, um sehr, sehr rasch zuzuordnen, woher kommt das, wer steckt dahinter. Mit großen Unsicherheiten noch, ob das hundertprozentig immer stimmt, ist fraglich. Wer sind die Angreifenden? Wie groß muss die Gruppe sein? Als ich das erste Mal ein ähnliches Szenario präsentiert habe, hieß es, da wird man jetzt zehntausende Soldaten brauchen. Und unendlich viele Waffen. Alle waren überrascht, als ich sagte, dafür genügen ein paar Dutzend schlaue Köpfe, ein bisschen Zeit, ein bisschen Geld – ein bisschen im militärischen Sinne. Keine hohen Summen. Und dann könnte man, wenn die Infrastruktur schlecht geschützt ist, sehr, sehr großen Schaden in kurzer Zeit anrichten. Das bedeutet aber auch, dass nicht nur große Staaten solche Angriffe vorbereiten können, sondern auch Gruppierungen, sogar Terrorgruppen. Wer sich einmal die Seite des IS angeschaut hat – das ist hochprofessionell gestaltet worden. Man muss also davon ausgehen, dass auch in diesen Reihen Hacker, kluge Köpfe dabei sind, die solche Szenarien überlegen könnten. Das heißt, offensive, aggressive Methoden sind in vielen Ländern in Vorbereitung. Ob und wann sie angewandt werden, das ist eine andere Frage.

August Reinisch, Professor für Völker- und Europarecht an der Universität Wien, Institut für Europarecht, Internationales Recht und Rechtsvergleichung, ist seit 2018 korrespondierendes Mitglied der Österreichischen Akademie der Wissenschaften.

THOMAS EITER

Man liest sehr viel darüber, was verschiedene Staaten auf diesem Gebiet an Tätigkeiten entfalten. Herr Reinisch, wie sieht hier die rechtliche Situation aus? Wir haben gehört, es gibt einen Verteidigungsfall und es gibt sozusagen nur gewöhnliche Kriminalität, die mit Strafverfolgung geahndet werden muss. Wie sieht es von juristischer Seite her aus?

AUGUST REINISCH

Ich wollte, ich könnte eine kurze Antwort geben. Vielleicht einleitend, falls jemand im Publikum kein Internet-Experte ist: Ich gehöre auch dazu. Ich habe mit großer Bestürzung dieses Video gesehen und frage mich auch, wie das in den Griff zu bekommen ist. Aber um auf die rechtliche Ebene zu kommen, wir haben gerade die Überlegungen aus einer Verteidigungsperspektive gehört, wie rüstet man sich gegen Cyberattacken. Im Vorfeld unserer Podiumsdiskussion habe ich auch etwas zögernd geantwortet und gesagt, das ist nicht primär eine völkerrechtliche, zwischenstaatliche Frage, sondern sehr häufig sind hier jene staatlichen Instrumente gefordert, die gegen kriminelle Tätigkeiten vorgehen.
Und das findet eine sehr schöne Entsprechung in der Ressortaufteilung in Österreich. Das Innenministerium ist für die innere Sicherheit zuständig und damit auch für die Durchsetzung strafrechtlicher Normen. Aber, und das ist ganz wesentlich, da wird es für uns Völkerrechtler interessant: Wir haben gerade gehört, was aus militärstrategischer Perspektive als Verteidigungsfall angesehen wird. Wir haben dazu ungefähr zehn Jahre lang im Völkerrecht eine spannende akademische Diskussion geführt. Sind die üblichen Regeln der Selbstverteidigung, des bewaffneten Angriffs, unter Berücksichtigung des Sicherheitsrats der Vereinten Nationen und seiner Befugnisse, des Rechts der bewaffneten Konflikte und dergleichen, hier anwendbar oder nicht? Oder ist das eben etwas ganz Anderes, weil es sich im sogenannten virtuellen Raum abspielt? Das Video hat meines Erachtens sehr gut illustriert, dass das, was vielleicht im Cyberspace virtuell einen Ausgangspunkt hat, dann sehr real in unserer unmittelbaren Umwelt Auswirkungen haben kann.
Und dann stellt sich die Frage: Wie reagieren wir darauf? Es herrscht

weitgehend Konsens darüber, dass ein Cyberangriff eine Intensität haben kann, die einem bewaffneten Angriff gleichzuordnen ist. Und dafür haben wir das klassische völkerrechtliche Instrumentarium, nämlich legitim Selbstverteidigung zu üben. Das ist noch nie geschehen, das ist auch aus guten Gründen noch nicht geschehen. Aber es gibt diese Möglichkeit. Wenn es heißt, Beeinträchtigung der Souveränität, dann muss man aufpassen. Es gibt sehr viele solcher Angriffe, die sich vielleicht gezielt gegen österreichische Interessen, gegen die österreichische Wirtschaft richten können. Damit ist aber noch längst nicht die Schwelle erreicht, um sagen zu können: Wir sind Opfer eines bewaffneten Angriffs im Cyberwar. Sondern vielleicht sind wir Opfer einer Souveränitätsbeschränkung, gegen die man mit verhältnismäßigen Gegenmaßnahmen vorgehen kann.

Wir sprechen im zwischenstaatlichen Bereich zwar davon, dass wir in der Lage sein müssen, einen angreifenden Staat zu identifizieren, gegen den wir uns dann entweder zur Wehr setzen oder Gegenmaßnahmen ergreifen. Aber eines der Hauptprobleme ist – und da ist wieder mein technisches Nichtwissen ein Hindernis – was Sie Attribution genannt haben, was wir im Völkerrecht Zurechenbarkeit nennen. Das ist genau dasselbe. Es wird immer von Gruppierungen gesprochen. Und dann rätselt man, ob diese im staatlichen Auftrag gehandelt haben oder geduldet wurden. Da muss man besonders aufpassen. Und da liegt die eigentliche Schwierigkeit, in diesen zwei rechtlichen Fragen: Legitimiert die Intensität, Gegenmaßnahmen oder sogar Maßnahmen der Selbstverteidigung zu ergreifen? Und wenn ja, gegen wen?

Wir haben ähnliche Probleme vor zwanzig Jahren diskutiert, nach 9/11, als es um terroristische Angriffe mit Zivilluftfahrzeugen gegangen ist – also nicht so, wie man sich einen Angriff bis dahin vorgestellt hatte. Aber das hat zur Verfestigung der Überzeugung geführt, dass ein Angriff nicht unbedingt mit konventionellen Waffen erfolgen muss. Und wenn wir hier sehen, dass man einen Cyberangriff so gestalten kann, dass er verheerende Auswirkungen hat, dann wird das ähnlich sein. Man wird darin je nach Intensität einen Angriff sehen können, gegen den Maßnahmen der Selbstverteidigung grundsätzlich zulässig sind.

Wir haben auch eine zweite interessante Parallele. Es war klar, dass der 9/11-Angriff nicht von einem staatlichen Akteur ausgegangen ist. Dann hat die verzweifelte Suche, sage ich jetzt einmal pointiert, der USA begonnen: Welcher Staat steht hinter dem Angriff? Und können wir Al-Qaida mit Afghanistan gleichsetzen oder nicht? Und das konnte man natürlich nicht so einfach. Aber ich möchte hier vielleicht nicht gleich anfangs zu viel Munition liefern.

THOMAS EITER

Vielen Dank für diese Einschätzung und diese Informationen aus rechtlicher Sicht. Man erkennt zunehmend diese Grauzone, die von bestimmten Beteiligten sehr gefördert wird, die auch in der konventionellen Konfliktführung ähnlich agieren: Dass versucht wird, nicht mehr offen Flagge zu zeigen, sondern bewusst offizielle Strukturen zu umgehen. Kehren wir aber nochmals auf die technische Ebene zurück. So wie auf der rechtlichen Ebene, die in einem gewissen Sinn ein Moving Target ist, weil sich ja alles schnell immer wieder verändert, ist es vermutlich auch auf der technischen Ebene. Es ist wahrscheinlich fast ein neues Wettrüsten, das sich da ergibt. Ist es ins-

besondere was die Angriffsszenarien angeht nicht so, dass sich diese ständig verändern? Welche Rolle spielt der technische Fortschritt dabei, dass mit neuen Bedrohungen gerechnet werden muss?

CARINA KLOIBHOFER

Natürlich ist es eine sehr schnelllebige Szene. Wobei schnelllebig auch relativ ist. Ich glaube, die ersten Ransomware-Angriffe wurden um 2010 herum bemerkt oder verzeichnet. Mittlerweile, 2019, zählen diese immer noch zu den häufigsten Angriffsformen, die wir haben. Schnelllebig ist bei zehn Jahren natürlich relativ. Man muss aber dazu sagen, dass natürlich die Grund-Ransomware noch vorhanden ist, wobei es mittlerweile über 700 verschiedene Ausprägungen gibt, die alle unterschiedlich agieren, alle unterschiedliche Verschlüsselungsalgorithmen verwenden und sich natürlich immer minimal weiterentwickeln. Was zur Folge hat, dass das, sobald das minimalst verändert wird, von Systemen eventuell nicht mehr so leicht zu erkennen ist. Beziehungsweise von den klassischen Systemen, wie man sie bisher kannte, die, wie zum Beispiel Ransomware Varianten, signaturbasiert nicht mehr eindeutig zu identifizieren sind. Wo man auf der Absicherungsseite zusätzliche Maßnahmen setzen kann und muss. Was mittlerweile schon der Fall ist, ist ganz einfach Anomaliedetektion in Netzwerken oder in den Systemen an sich. Das heißt, es gibt Systeme, die mittlerweile lernen, was ist mein normales Verhalten, was ist mein normaler Netzwerk-Traffic, was ist normales Vorkommen. Dadurch können dann auch solche leichten Veränderungen (zum Beispiel im Verhalten der Ransomware) großen Impact haben. Weil sie – die Detektionsmechanismen – einfach davon weggehen, jetzt genau auf die Signatur zu gehen oder genau auf die eine Ausprägung der Malware oder des Angriffs. Hin zu, okay, ich kenne mein normales Verhalten und kann dann aufzeigen, wenn etwas vom normalen Verhalten abweicht. Das heißt, es gibt auch immer ein leichtes Wettrennen, wer schneller ist. Die Angreifenden oder diejenigen, die sich absichern oder – in größeren Dimensionen – sich verteidigen möchten.

THOMAS EITER

Welche Rolle spielt hier künstliche Intelligenz? Wird es zu einer Vergrößerung der Bedrohung durch den Einsatz künstlicher Intelligenz kommen?

CARINA KLOIBHOFER

Ich glaube, KI ist mittlerweile in aller Munde. Natürlich auch bei den Cybersicherheitssystemen. Einerseits bei der Abwehr oder Absicherung, jetzt eben auch bei der Anomaliedetektion, wo sehr stark auf KI oder Machine Learning fokussiert wird, also die Maschinen an sich lernen zu lassen und nicht mehr ein definiertes Regelwerk vorzugeben. Theoretisch könnte aber ein sehr gezielter Angriff, wenn er geschickt genug gemacht ist, sich wiederum solche Mechanismen zunutze machen und versuchen, dieses normale Verhalten möglichst gut nachzuahmen und dann ganz gezielt einzusetzen. Wobei mir persönlich ein Angriff in dieser Dimension noch nicht bekannt wäre, weil das natürlich nochmals ein größerer Ressourcenaufwand ist. Eben weil der oder die Angreifende zunächst das normale Verhalten

dieses Netzwerks, der Organisation, der kritischen Infrastruktur, lernen müsste, um sich dann dort unbemerkt zu etablieren.

DIETMAR MANDL

Wir beschäftigen uns natürlich genauso mit der Angreiferseite. Generell sind dabei drei Faktoren zu beachten: die zeitliche Komponente sowie die personellen und die monetären Ressourcen der Angreifenden. Wenn nur der monetäre Aspekt im Vordergrund steht, reicht es aus, eine „Standard-Ransomware" zu nutzen, diese an eine Million Leute zu versenden und zu hoffen, dass jeder zehnte diese ausführt. Dies lässt sich relativ leicht und ohne großen Aufwand durchführen. Diverse Tools oder Services dafür gibt es kostenlos oder kostengünstig im Internet zu beziehen.
Die eigentliche Frage ist jedoch, was der Akteur bzw. die Akteurin erreichen möchte. Was ist das eigentliche Ziel des Angriffes? Wer auf rein monetäre Aspekte abzielt, wird sich wahrscheinlich leichtere Ziele aussuchen als eine große Behörde, einen Staat oder eine kritische Infrastruktur, weil diese tendenziell besser geschützt sind, mehr Ressourcen und einfach ein höheres Sicherheitsniveau haben. Warum sollte ich in den Bunker eindringen, wenn ich beim Nachbarn über den Zaun springen und durch das offene Fenster ins Haus einsteigen kann?
Wenn es Richtung Cyberwar geht, sind andere Motive relevant und auch die drei genannten Faktoren sind in ausreichendem Ausmaß vorhanden. Hier könnten wir wahrscheinlich auch im Fokus von möglichen Angriffen stehen. Als Betreiber einer kritischen Infrastruktur setzen wir natürlich umfassende Maßnahmen, um es Angreifern aller Art so schwer wie möglich zu machen. Neben technischen Schutzmaßnahmen sind auch organisatorische und prozessuale Maßnahmen notwendig, um ein entsprechend hohes Schutzniveau zu gewährleisten.
Ein Fokuspunkt ist etwa der normale E-Mail-Empfang. Hier sind sowohl Sensibilisierungsmaßnahmen der Mitarbeiterinnen und Mitarbeiter als auch technische Filterungsmaßnahmen notwendig. Weiters sind Architektur- und Designentscheidungen zu treffen, wie beispielsweise das eigene Netzwerk aufgebaut ist beziehungsweise wie Netzwerkübergänge gestaltet werden. Wichtig ist ein ausgewogenes Maßnahmenbündel in den Bereichen Prävention, Detektion und Response, also Reaktion.

THOMAS EITER

Welches Spezialwissen müsste man denn haben, um einen größeren Blackout zu bewerkstelligen? In Ihrem Bereich, also speziell im Energiebereich – ist das etwas, das man relativ einfach machen kann? Oder muss man da schon tiefes Wissen haben und das entsprechend einsetzen können?

DIETMAR MANDL

Es sind viele verschiedene Aspekte. Man kann das jetzt nicht konkret an einer Person oder einer speziellen Ausbildung festmachen. Es stellt sich wieder die Frage, wer mir da gegenübersitzt. So wie Herr Unger vorher schon erwähnt hat, reichen ein Dutzend oder ein paar Dutzend schlaue Leute aus unterschiedlichsten Disziplinen. Dann ist es wahrscheinlich nur eine Frage der Zeit, abhängig von den finanziellen und technischen Ressourcen.

THOMAS EITER

Bei diesem Wettlauf zwischen Angriff und Abwehr, ist man da in der Lage Schritt zu halten?

WALTER UNGER

Der Angreifer ist natürlich, wie in vielen Bereichen, im Vorteil. Der kann sich jeden Tag etwas Neues einfallen lassen. Und der Verteidiger ist in der Reaktionssituation.
Warum ist es möglich? Warum kann sich jemand jeden Tag etwas Neues einfallen lassen? Weil die Software, die uns allen heute verkauft wird, dem Teufel zu schlecht ist. Das BSI (*Bundesamt für Sicherheit in der Informationstechnik, Red.*) entdeckt jeden Tag drei schwerwiegende Schwachstellen und Dutzende weniger schwerwiegende Schwachstellen in der Software, die heute am Markt ist. Das heißt, es werden in jedem sicheren Haus Löcher zu finden sein, in die man hineinkriechen kann und die man attackieren kann. Das ist ein Feld, wo der oder die Einzelne nichts unternehmen kann. Hier muss durch den Staat, und überregional im EU-Rahmen, dagegen vorgegangen werden. Das heißt, man muss die Lieferanten zwingen, etwas Ordentliches zu produzieren. Software, die einen Elchtest aushält und nicht sofort attackierbar wird.
Das Gleiche gilt für die Algorithmen der KI. In aller Regel sind diese nicht ausgetestet, niemand weiß, wie sie in speziellen Situationen reagieren werden. Oder man führt Internet of Things (IoT) ein – in Milliarden. Nächstes Jahr haben wir wahrscheinlich schon 50 Milliarden vernetzte Geräte. Und nicht alle sind auf Sicherheit ausgelegt und so billig, dass man gar kein Geld dafür verwenden kann, um sie sicher zu gestalten. Wir bauen aber Smart Homes, Smart Cities, Smart Meter, smarte Autos. Ob die dann wirklich funktionieren – oder wie sie auf leichte Störungen reagieren –, sieht man dann erst im Anlassfall. Das heißt, wir sind deshalb verwundbar, weil wir uns auf eine IT abstützen müssen, die von Haus aus schlecht gebaut ist. Erfreulicherweise gibt es seit zwei Jahren Universitätsprogramme, die auf sicheres Programmieren ausgelegt sind. Weniger erfreulich ist, wenn man sich durchliest, was die Ziele sind. Man will erreichen, dass man Programme baut, die nur 0,5 Fehler bei 1.000 Programmzeilen haben. Wenn wir das auf die Bremsschläuche von unseren Autos umlegen, dann platzt dann jeder zweitausendste Bremsschlauch irgendwann auf der Autobahn, wenn wir gerade zu schnell fahren. Das ist die eine Dimension. Wenn man aber sieht, wie viele Programmzeilen so ein komplexes Programm hat – das Auto, das uns da selbst kutschiert –, nämlich hundert Millionen Programmzeilen, kann man sich ausrechnen, wie viele Schwachstellen hier verborgen sind, die vielleicht noch gar keiner kennt und die erst durch Unfälle oder Attacken bekannt werden.
Umgekehrt ist es am Schwarzmarkt eine sehr gut bezahlte Tätigkeit, wenn man „Zero Days“ anbieten kann. Sprich, jemand findet eine solche Schwachstelle – dafür werden bis zu siebenstellige Beträge gezahlt – und ein anderer baut daraufhin eine Malware und veranstaltet einen Angriff, entweder um Geld abzuzocken oder aber auch, um Geheimnisse auszuspionieren oder eine Cyberattacke im sicherheitspolitischen Bereich vorzubereiten. Das heißt, eine große Problematik ist, wenn die Infrastruktur, auf die wir uns verlassen, schlecht ist. Diese muss also deutlich verbessert werden. Vielleicht sollte man ein Haftungsrecht einführen, wie es für jedes andere Produkt gang und

gäbe ist. Im Umkehrschluss, wenn ich jetzt weiß, wir haben nur schlechte Software zur Verfügung, was tue ich dann bei kritischen Infrastrukturen? Wie ist es zum Beispiel mit der Steuerung der Stromversorgung? Hier werden wir dann hoffentlich die Steuersoftware nicht kaufen, sondern selbst entwickeln, sie möglichst gut testen und, was noch wichtiger wäre, die Software nicht mit dem Internet oder mit anderen unsicheren Systemen verbinden.

Das ist der Fehler, der in den letzten 20 Jahren gemacht wurde. Alle wollten vernetzt sein. Was ist das Billigste? Das Internet, das kostet nichts. Es wird zur Verfügung gestellt und keiner denkt darüber nach, was da passiert. Und nachdem immer mehr vernetzt wird und die Wechselwirkungen de facto unbekannt oder gar nicht austestbar sind, sind wir auch hier angreifbar. Wichtig wäre daher, schützenswerte Systeme zu entkoppeln, zu entnetzen, und dann möglichst zuverlässige Software, die man vielleicht auch selbst entwickelt hat, einzusetzen.

THOMAS EITER

Die Entwicklung von korrekter Software ist also theoretisch ein alter Traum, der aber nicht immer umsetzbar ist. Es gibt da große Barrieren, die eine praktische Umsetzung verhindern. Mit gewissen Fehlern wird man wahrscheinlich leben müssen. Dass man die Fehlerrate reduzieren kann, indem man entsprechende Auflagen und Qualitätszusicherungen zwingend vorsieht, ist etwas, was man anstreben kann. Aber dass alles absolut fehlerfrei sein wird, das ist wahrscheinlich zu verwegen, als dass man davon träumen oder sich dies erhoffen kann. Ich meine, mit der Sicherheit ist es vielleicht so – wenn ich auf das zurückkomme, was schon gesagt wurde –, dass man zwar versucht, die Tür eines Hauses fest verschlossen zu halten oder eine Sicherheitstür einbaut, aber dann das Fenster daneben sperrangelweit offenstehen lässt.

CARINA KLOIBHOFER

Ich glaube, die richtige Antwort auf diese Frage gibt es nicht. Es ist tatsächlich so, wie es einem zu Hause passiert, dass man die Haustür zusperrt, das Fenster aber offenstehen lässt. So kann es auch jeder Organisation passieren. Nun kann dies passieren, weil der Fokus im Vordergrund steht: Was sind meine kritischen Assets? Und dann droht natürlich auch in diesen Bereichen die Gefahr, eine gewisse Betriebsblindheit zu entwickeln. Oder Systeme zu haben, bei denen man sich gar nicht bewusst ist, dass es hier Schwachstellen gibt. Deshalb ist es wichtig, dass man versucht – auch aus Organisationssicht, aus Schutzsicht –, Fachleute aus unterschiedlichen Disziplinen zusammenzubringen, die fähig sind, die vorhandenen Systeme wirklich ganzheitlich zu analysieren. In Zukunft, glaube ich, ist für jeden Hacker, jede Hackerin die größte Hürde, dass mittlerweile auch in diversen Richtlinien und Gesetzen „Security by Design“ ganz konkret verlangt und angeführt wird. Software und Systeme müssen mittlerweile mit dem Fokus auf „Security by Design“ entwickelt werden. Das heißt, der erste Prozessschritt, den ich machen muss, wenn ich ein neues System oder eine neue Software entwickle, ist der, auch an die Sicherheit zu denken. Das ist eine große Weiterentwicklung, verglichen mit den alten Systemen, die teilweise noch im Einsatz sind – und

das macht dann hoffentlich auch wieder den Hackern und Hackerinnen das Leben schwerer.

DIETMAR MANDL

Das ist ein wichtiger Punkt. Security ist keine Einmalsache, die man einmal im Unternehmen einführt oder in ein Produkt einbaut. Security ist ein fortdauernder, wiederkehrender Prozess, den man ständig durchleben, verbessern und weiterentwickeln muss. Aus meiner Sicht ist die große Problematik dabei die Komplexität. Durch rasante Weiterentwicklungen und den Einsatz von neuen Technologien ist ein entsprechendes Reagieren auf Änderungen der Rahmenbedingungen enorm wichtig. Aufgrund der Komplexität ist es daher aus meiner Sicht wichtig, für eine gewisse Transparenz im Unternehmen zu sorgen. Wie kann ich mein System bestmöglich abschotten beziehungsweise abkoppeln? Wo brauche ich Schnittstellen zu anderen Systemen? Wer greift wie auf meine Systeme zu? Je besser mein Verständnis zu den Vorgängen im Unternehmen ist, desto leichter lassen sich unerwünschte Zustände oder Zugriffe erkennen.

In den letzten Jahren haben sich auch entsprechende gesetzliche Grundlagen entwickelt, welche Sicherheitsmaßnahmen für kritische Infrastrukturen vorsehen. Allein das per Gesetz vorzuschreiben, ist aber zu wenig. Man muss das Sicherheitsniveau als Unternehmen ganzheitlich weiterentwickeln und sich ständig an die Umgebungsbedingungen anpassen.

THOMAS EITER

Inwieweit würde denn da der Faktor Mensch eine Rolle spielen? Oder würde dieser für Sicherheitsbedenken keine Rolle spielen?

WALTER UNGER

Gott sei Dank steuern wir unsere IT derzeit noch selbst. Das kann in naher Zukunft anders sein, etwa dass Software und Roboter und KI uns steuern. Noch haben wir es auch bis zu einem gewissen Maß in der Hand, unsere Mitarbeiterinnen und Mitarbeiter so auszubilden und zu sensibilisieren, dass sie möglichst wenige Fehler machen. Dass ihnen klar ist, was passieren kann, dass sie mit den Geräten ordentlich umgehen, ein vernünftiges Passwort setzen und dieses auch regelmäßig wechseln zum Beispiel. Oder dass sie nichts ausplaudern an den Geräten oder sich nicht in sozialen Foren produzieren und dabei Betriebsgeheimnisse offenbaren. Also alles Dinge oder Pläne, die für einen Angreifer bzw. eine Angreiferin interessant wären.
Mitarbeiterinnen und Mitarbeiter spielen nach wie vor eine zentrale Rolle. Sie müssen entsprechend vorbereitet werden. Das reicht aber nicht, wenn die Chefetagen nicht sensibilisiert sind, nicht verstehen, wie es unlängst der Generaldirektor einer großen österreichischen Bank gesagt hat, was eine Bank in der Zukunft ist: ein Riesen-Rechenzentrum. Das ist heute schon so. Schaltet man die Computer ab, gibt es die Bank nicht mehr. Mit oder ohne Personal davor und dahinter – dann ist sie tot. Das heißt, die Leute, die daran arbeiten, müssen wissen, wie es geht. Und die Chefetage muss verstehen, wie wichtig diese Sicherheit für das Gesamtunternehmen ist. Ganz abgesehen davon, dass mit den neuen Technologien und Trends wie KI und IoT jedes Unternehmen darüber nachdenken muss, wo seine Zukunft liegt. Man liest Statistiken oder Vorhersagen, wo Unternehmensberater sagen, 50 Pro-

zent der Unternehmen, die heute an der Weltspitze stehen, werden in fünf Jahren nicht mehr dort sein, weil sie die Digitalisierung verschlafen haben. Das ist dann genauso schlecht. Also, das ist ein zentrales Thema, wie das Beispiel großer Versicherungsunternehmen zeigt, die vor zehn Jahren Cyberrisiko noch gar nicht versichert haben, weil es noch kein Risiko war. Und heute, bei Lloyds etwa, rangiert Cyberrisiko als Toprisiko neben dem operationellen Risiko. Das heißt, in zehn Jahren von null an die Spitze, einfach deshalb, weil es so wichtig für alle Unternehmen ist. Aber nicht nur für die Unternehmen, speziell bei hoch technologisierten Staaten wie Österreich gilt dies auch für den Gesamtstaat.

THOMAS EITER

Hat Österreich überhaupt die Fachkräfte, um das stemmen zu können? Sie haben gesagt, wir brauchen gut ausgebildetes Personal, das sich dessen bewusst ist, damit wir das Risiko minimieren können. Sie werden sicher auch für Ihren Stab gut ausgebildete Mitarbeiterinnen und Mitarbeiter brauchen?

WALTER UNGER

Wenn man hier die Zukunft gewinnen will, dann brauchen wir gutes Personal und müssen dort am meisten investieren. Jetzt haben wir in Österreich zwei Probleme. Wir haben viel zu wenig Personal. Ich habe eine aktuelle Aufstellung gelesen, wonach in Österreich jetzt, im Jahr 2019, 34.000 IT-Fachkräfte fehlen. Also nicht nur für IT-Sicherheit, sondern für den gesamten Bereich. Vor einer Woche hat ein Manager gesagt, wir bräuchten jedes Jahr 15.000 neue IT-Fachkräfte. Es werden aber nur 1.500 pro Jahr von unseren Fachhochschulen und Universitäten fertig ausgebildet. Und wir leben hier in einem großen Konkurrenzkampf mit den Nachbarstaaten, mit den USA und anderen Ländern, die immer wieder äußerst attraktive Angebote machen. Nehmen Sie beispielsweise die Fachhochschule Hagenberg in Oberösterreich, dort haben wir über zehn Jahre einen Fachhochschullehrgang für unser Personal durchgeführt. Die Studierenden in Hagenberg haben in aller Regel schon im fünften Semester ein fixes Jobangebot. Gut die Hälfte der Absolventinnen und Absolventen geht sofort ins Ausland, nach Deutschland oder in die Schweiz oder noch weiter weg. Und sie gehen natürlich für unseren Arbeitsmarkt verloren. Ich befürchte, dass der Nachwuchs nicht deutlich steigen wird und dass wir daher – schon beginnend im Schulalter – große Anstrengungen unternehmen müssen, damit unsere nachkommende Generation erstens mit den Systemen nicht nur sicher leben, sondern zweitens diese auch noch beherrschen kann. Sonst werden wir vielleicht einmal froh sein, dass der Algorithmus das macht, was wünschenswert ist.

STATEMENT PUBLIKUM 1

Ich habe die Statements von Herrn Unger betreffend Softwaresicherheit genossen. Die alten Systeme, die alle 14 Tage ein Update brauchen. Jetzt aber die Frage: Halten Sie es für sinnvoll, wenn die EU im Rahmen eines EU-Projektes eine komplett neue, sichere Softwareumgebung schaffen würde, mit der wir leben und in Zukunft sicherer sein können?

WALTER UNGER

Wir haben in Europa die Marktwirtschaft. Es wird nicht so einfach sein,

das von staatlicher oder von EU-Seite zu triggern. Aber ich glaube, Sie meinen das, was ich auch denke. Nämlich die Rahmenbedingungen zu schaffen, dass sich Unternehmen in Europa entwickeln und europäische Produkte entstehen können, die auch entsprechende Anforderungen, die wir alle stellen, erfüllen. Dazu vielleicht auch Zahlen. Die Wirtschaftskapitäne sagen, Europa hat zu wenig Risikokapital, damit der IT-Markt entsprechend konkurrieren kann mit den USA oder China. Die USA stellen im Jahr etwa 100 Milliarden Dollar Risikokapital zur Verfügung und können damit natürlich jede Idee, die irgendwie gut ausschaut, entsprechend fördern. China investiert 60 Milliarden und die EU nur 30 Milliarden – der reichste Wirtschaftsraum stellt somit ganz klar am wenigsten zur Verfügung. Und das bedeutet auch, dass unsere Unternehmen sehr oft von den Internetgiganten aus den USA gekauft werden. Apple hat 250 Milliarden in der Kasse, weiß nicht wo es investieren soll und kauft alles auf, was irgendwie zukunftsträchtig aussieht. Und die anderen detto. Es wäre daher notwendig, dass die EU hier Rahmenbedingungen schafft, damit mehr Risikokapital zur Verfügung steht. Damit dieses auch investiert wird, sollte in gleichem Ausmaß auch in die Wissenschaft, in die Forschung investiert werden. Damit einfach mehr neue Ideen entwickelt werden können.

STATEMENT PUBLIKUM 1

Ich würde noch weitergehen. Ich denke hier nicht an Risikokapital, denn unsere Konkurrenzsysteme in China, den USA oder dergleichen sind ja teilweise aus militärischen Bereichen heraus entstanden, die zu hundert Prozent vom Staat bezahlt worden sind. Kein frei finanziertes System kann da konkurrieren. Da müsste doch eigentlich ein sicheres System für die EU-Bürgerinnen und Bürger von der EU selbst geschaffen werden.

WALTER UNGER

Ich glaube, das kann man nur bestätigen, sowohl in den USA als auch in China wird sehr viel aus den Forschungsbudgets des Militärs oder anderer Institutionen bezahlt und möglich gemacht. Es freut mich, dass Sie für höhere Militärbudgets sind. Aber Fakt ist auch, die USA gaben 650 Milliarden Dollar für ihr Militär im Jahr 2019 aus, das ist mehr als ganz Europa zusammen. Weit mehr. Also da gibt es Ungleichgewichte. Und hier können wir als kleines Österreich nur mitinitiieren, Verbündete suchen und im EU-Rahmen dafür eintreten. Vielleicht mit einem künftigen EU-Budgetkommissar, der da etwas bewegen kann. Das wäre die richtige Richtung, es muss aber nicht beim Militär angesiedelt sein.

THOMAS EITER

Also man kann vielleicht noch ergänzend dazu sagen, es ist zunehmend für die Wissenschaft auch ein Problem, dass globale private Player wie Google, Amazon und andere Firmen führende Köpfe abwerben, weil sie einfach die Mittel haben. Zum einen nicht nur, um die Gehälter zu bezahlen, sondern auch, um die Forschungsbedingungen zu schaffen, die sehr anziehend für Topwissenschaftlerinnen und -wissenschaftler sind. Und auf diese Art und Weise natürlich dann auch einen Technologievorsprung erwerben. Das heißt, Europa wird sich überlegen müssen, hier Maßnahmen zu ergreifen. Man

hat immer wieder von einer Internetsteuer, Digitalisierungssteuer gesprochen. Wenn man hier etwas erreichen könnte, dann würde man durchaus auch über Mittel verfügen, die man direkt in Forschung und Entwicklung stecken könnte. Die dazu beitragen würden, uns zunächst auf technischer Ebene besser entwickeln zu können. Das wäre ein wichtiger Schritt. Mit einigen Milliarden Euro im Jahr könnte man bereits einige größere Projekte finanzieren, die dann in die Richtung gehen, die Sie genannt haben. Also dass man nicht nur versucht, es aus Steuergeld zu finanzieren, sondern auch jene, die vom momentanen Zustand profitieren, entsprechend besteuert.

GEORG BRASSEUR

Ich möchte wieder auf das Thema Blackout durch Cyberwar zurückkommen. Ist es notwendig, das Insiderwissen eines Energieversorgers zu haben, um ihn angreifen zu können? Muss man vielleicht sogar physischen Zugang zu seinen Anlagen haben, um einen Angriff starten zu können? Oder geht das quasi wirklich aus der Ferne, ohne Insiderwissen, ohne physischen Zugang?

DIETMAR MANDL

Das ist eine gute Frage. Wir haben es vorher von Herrn Unger schon gehört. Jede Industrie setzt auf Informationstechnologie. Sprich, es funktioniert nichts mehr ohne Computer. Für unterschiedliche Tätigkeiten, vom Messen bis zum Steuern, wird irgendwo ein elektronisches Gerät eingesetzt, welches de facto ein Computer ist. Der Punkt ist hier: Wie weit lasse ich es zu, dass die Geräte miteinander verbunden sind? Wie weit lasse ich zu, dass die Systeme von der Ferne erreichbar sind? Und welche Schutzmaßnahmen setze ich? Man kann durchaus sagen, dass alles irgendwie elektronisch erreichbar ist. Also wenn man als Akteur bzw. als Akteurin genügend Zeit, monetäre und personelle Ressourcen hat, ist es nur eine Frage der Zeit, dass man zu den kritischen Systemen vordringt. Daher ist notwendig, die richtigen Schutzvorkehrungen zu treffen, um so früh wie möglich Angriffsversuche zu erkennen und schnellstmöglich darauf reagieren zu können.

STATEMENT PUBLIKUM 2

Wir haben jetzt von Cyberkriminalität gehört. Meine Frage wäre nun: Wie groß ist die Zeitspanne, die zum Beispiel in Österreich notwendig ist, um wieder zu einem normalen Stromversorgungszustand zu kommen? Wir haben im Film gehört, 48 Stunden sind gerade noch kritisch, eine Woche ist verheerend. Gibt es dazu Szenarien und Antworten, wie es in der Realität ausschaut? Wie schnell – nicht bei physikalischer Zerstörung, sondern bei einem reinen Cyberangriff – kann das dann wieder zum Laufen gebracht werden?

DIETMAR MANDL

Einen konkreten zeitlichen Faktor kann ich Ihnen nicht nennen. Es kommt auf das entsprechende Szenario an. Dabei ist dann die Frage, wie schnell ich die eigentliche Ausfallursache identifizieren kann. Im Falle eines Blackouts wird man versuchen, das Stromnetz Zug um Zug wiederaufzubauen, um langsam wieder hin zu einer vollständigen Versorgung zu kommen. Man kann keine pauschale Antwort geben, weil es wie gesagt vom jeweiligen Szenario abhängt.

STATEMENT PUBLIKUM 3

Wie sieht es mit Vorbereitungen gegen Hybridangriffe aus? Dass zum Beispiel ein Bereitschaftstechniker der Austrian Power Grid in Gewalt genommen wird, beziehungsweise dessen Familie. Und somit aus einem Outsiderangriff ein Insiderangriff gemacht wird.

DIETMAR MANDL

Das Thema Insiderattacke hat man in jedem Unternehmen, das kann man nie gänzlich ausschließen. Jeder Mensch ist wahrscheinlich käuflich. Es kommt auf die Geldsumme und die Motivation an. Die Frage ist, wie man sich tatsächlich davor schützen kann. Hier gibt es keine pauschale Antwort.

STATEMENT PUBLIKUM 3

Die Frage zielt darauf ab, ob es Vorbereitungen gibt, die eben genau diesen Fall verhindern, dass das Personal entsprechend mit Alarmworten gebrieft ist. Da gibt es einige Möglichkeiten. Sind diese vorbereitet oder würde uns das komplett unvorbereitet treffen?

DIETMAR MANDL

Es würde uns jetzt nicht komplett unvorbereitet treffen. Es sind unterschiedliche Sicherheitsvorkehrungen vorgesehen, um den unterschiedlichen Bedrohungen vorzubeugen.

STATEMENT PUBLIKUM 4

Vielen Dank für die sehr guten Beiträge und ein spannendes Thema, das ich für mich selbst versucht habe zu übersetzen: Ein umfassender Stromausfall durch Krieg auf virtueller/digitaler Ebene – wäre es übersetzt auf Deutsch. Und für mich stellt sich hier die Frage, wie realistisch ist es, nur einen Cyberwar zu haben. Warum? Weil, wenn ich Krieg führe, und alle großen Nationen oder alle, die sich dafür halten und derzeit versuchen, bewaffnete Konflikte vom Zaun zu brechen, nutzen das nur als eine Ebene. Der Cyber Command ist nichts anderes als die Marine, als die Luftwaffe, als die Armee. Das heißt, ich werde nie einen Krieg nur mit einer Waffengattung führen. Ich werde eine besonders nutzen, weil ich vielleicht die anderen Möglichkeiten nicht habe. Aber das bringt mich zu dem Thema, und ich bin hier ganz bei Oberst Unger, dass wir zum Beispiel sichere Software brauchen. Aus verschiedensten Gründen. Schon aus Haftungsfragen. Der Jurist in mir sagt das. Allerdings finde ich es etwas schwierig, eine auf Optimierung ausgelegte Friedensökonomie auf Vulnerabilität durch einen kriegerischen Angriff abzuklopfen. Natürlich verliere ich da. Das ist das Gleiche, wie wenn ich frage: Blackout durch Air War? Da können wir uns auch nicht wehren im Moment, weil wir nicht darauf vorbereitet sind, weil dieses Szenario bei uns nicht vorkommt. Und für alles bräuchten wir einen zeitlichen Vorlauf und vor allem sehr viel Geld. Das Thema hatten wir auch schon. Meine konkrete Frage ist: Wenn das Ganze schon jetzt eingesetzt wird, warum brennt in der Ukraine noch das Licht?

AUGUST REINISCH

Ich habe diese Diskussion mit großem Interesse verfolgt, weil sie zeigt, dass wir von Cyberwar sprechen, aber in Wahrheit Cyberkriminalität meinen. Wir sprechen in erster Linie von nichtstaatlichen Akteuren, Kriminellen, die Handlungen vornehmen, und davon, wie schütze ich

mich als Unternehmen auch davor, dass womöglich eigene Beschäftigte erpresst werden, um dann auch wieder schädigend gegen die Daten des Unternehmens etc. vorzugehen. Das war für mich das Interessanteste, zu hören, dass die Überlegungen etwa des Bundesheeres nicht primär darauf abzielen: Wie schlagen wir militärisch zurück? Sondern darauf: Wie schützen wir uns? Und das ist ja genau das Interessante daran, dass uns allen bewusst ist, dass wir zwar unter Umständen, wie ich das eingangs skizziert habe, rechtlich davon sprechen können, dass es sich um einen Cyberwar handelt und wir damit in einem bewaffneten Konflikt sind, das aber meistens nichts bringt. Es geht nicht darum, Selbstverteidigung zu üben und das Recht bewaffneter Konflikte zur Anwendung zu bringen, sondern es geht im Wesentlichen darum, möglichst rasch Infrastruktur wiederherzustellen, um den Schaden zu begrenzen.

Das zeigt dann auch gleichzeitig eine sehr interessante Debatte, die wir im Völkerrecht in den letzten zwei Dezennien hatten. Als das Internet aufgekommen ist, hat man gedacht, das ist jetzt endlich einmal ein rechtsfreier Raum. Und alle waren ganz euphorisch. Wunderbar, das unterliegt nicht mehr staatlicher Souveränität und braucht nicht mehr geregelt zu werden. Und hier haben wir die Möglichkeit, dass Individuen sich frei entfalten und Meinungsfreiheit weltweit garantiert wird. Man hat dann relativ rasch gesehen, dass es da doch erstaunliche Grenzen gibt, weil ganz einfach der Zugang zu Internetdomänen technisch geregelt werden musste. Das erfolgt über ICANN (*Internet Corporation for Assigned Names and Numbers, Red.*), eine amerikanische Corporation, die natürlich bestimmte Regeln befolgt, nach denen die einen zugelassen und andere nicht zugelassen werden. Das war in etwa die erste Debatte. Und mit den Missbrauchsmöglichkeiten, die es im Internet allgemein gibt, ist dann die Euphorie des rechtsfreien Raums abgeflaut.

Ein zweiter Entwicklungsschritt der völkerrechtlichen Debatte zur Regelung des Internets war dann vor allem einer, wo es um Ressourcenaufteilung ging. Die Entwicklungsländer sind gekommen und haben gefragt: Wieso wird alles von westlichen Staaten dominiert? Wir müssen für eine gerechte Aufteilung dieser Ressource sorgen. Ähnliches hatten wir vor Jahrzehnten schon im Seerecht und im Weltraumrecht: Aufteilung der Ressourcen. Und erst jüngst, erst so in den letzten zehn Jahren, gab es wieder einen Paradigmenwechsel. Dieser Raum der Freiheit, der Cyberraum, ist gleichzeitig etwas, das uns bedrohen kann – wie im Eingangsvideo gezeigt. Stuxnet wurde erwähnt. Estland war vor gut zehn Jahren auch einem Cyberangriff ausgesetzt, der dazu führte, dass wesentliche Regierungsfunktionen nicht möglich waren, weil Computer großflächig lahmgelegt waren. Man hat sich dann überlegt: Wie können wir darauf reagieren? Man erhofft sich vom Recht oft Folgendes: Das sind einmal die Spielregeln und dann fangen wir an zu spielen. In Wahrheit fangen alle schon längst an zu spielen und wir müssen dann versuchen, rechtliche Rahmenbedingungen zu schaffen. Die Technik ist uns immer voraus und wir versuchen irgendwie Antworten zu finden. Und es ist das Strafrecht, das langsam reagiert und sagt, es gibt eben neue Straftatbestände, die europaweit und weltweit eingeführt worden sind, als Reaktion. Es gibt die Überlegungen, wie können wir völkerrechtlich darauf reagieren, gleichzeitig eben immer mit einer meines Erachtens sehr willkommenen Zurückhaltung. Denn solange ich nicht weiß, wer mich

angegriffen hat und womit und gegen wen ich jetzt in welcher Art und Weise reagiere, muss man hier sehr vorsichtig sein.

WALTER UNGER

Ich glaube, ich sollte noch etwas dazu sagen, warum das Licht in der Ukraine noch brennt.
Das genau zu beurteilen, wird von hier aus schwer sein. Denn wir kennen die strategischen Überlegungen und Absichten Russlands ja nicht, oder? Das wissen wir nicht, warum das dort so ist. Und auf der anderen Seite wissen wir nicht genau, wie gut die Ukraine mittlerweile ihre Netze schützt. Denn sie haben schon einmal einen großflächigen Angriff mit hunderttausenden Betroffenen erlebt, um die Weihnachtszeit 2016, glaube ich, war das. Wo sie mehr als 48 Stunden, gerade dann, wenn der Truthahn im Backofen glühen sollte, keinen Strom hatten. Also warum? Das ist aber eine gute Frage, da kann man darüber nachdenken. Vor allem sollte man das den Sicherheitspolitikern mitgeben, damit sie analysieren können, was die strategischen Absichten dahinter sind. Aber die Frage zielt auch darauf ab: Wie sollte ein Prozess zum Schutz der eigenen Infrastruktur aufgesetzt sein? Und da gehört sicher dazu, dass man lange im Vorhinein schon im Frieden daran arbeitet. Weil jeder, der sich mit Angriffen beschäftigt, weiß, dass die jederzeit beginnen können. Jederzeit. Von null bis 24 Uhr. Da gibt es genug Beispiele. Der Kommunikationsanbieter A1 wurde von Freitag auf Samstag um Mitternacht attackiert, sechs Tage lang. Andere auch am Wochenende. Die Freunde, die unsere Türkeipolitik nicht so gutgeheißen haben, haben uns immer am Wochenende attackiert. Da haben wir gesagt, das sind so Feiertagscyberkrieger. Wahrscheinlich waren es Berufstätige, die nur am Samstag, Sonntag Zeit dafür hatten. Also es kann jederzeit losgehen. Das heißt, wir müssen uns so aufstellen und immer mitbedenken, dass wir nicht unverwundbar sind. Prävention, ja? Dazu gehört, dass wir ständig beobachten, was spielt sich denn im Cyberraum ab. Da macht das Militär sehr viel, aber auch andere. Und dass man eine Frühwarnung generiert. Das wissen wir alle, es geht sehr schnell im Cyberbereich. Das heißt, es geht oft um Millisekunden oder Sekunden. Wenn es automatisiert ist, funktioniert das. Verteidigung muss teilweise auch automatisiert werden.

Dann geht es darum, dass man schnell seine Abwehrkräfte verstärkt und die Einsatzbereitschaft hochfahren kann. Damit meine ich nicht nur das Militär. Auch ein Unternehmen muss schnell in der Lage sein, zu reagieren. Wenn man so einem Verschlüsselungstrojaner zuschaut, das dauert ein paar Sekunden und die ganzen Datenbestände sind verschlüsselt. Dann hat man nur mehr die Möglichkeit, tief in die Tasche zu greifen oder zu sagen, das war es, wir haben die Daten für die letzten Monate nicht mehr, weil wir sie nicht ordentlich gesichert haben. Also in der Prävention, in der Vorbereitung auf das, was passieren kann, liegt das Erfolgsgeheimnis. Wir müssten so gut geschützt sein, als Teil des Cyber-Power-Konzeptes, dass wir gar nicht in die Knie gezwungen werden können. Wir haben vielleicht Schäden, das tut weh, aber sie sind nicht vital. Und wenn Schäden eintreten, dann sollten wir eine Fähigkeit haben, möglichst rasch den Normalzustand wiederherzustellen. Der Strom geht aus und die APG sorgt dafür, dass spätestens zu Mittag wieder alles läuft. Also drei, vier Stunden später. Länger dürften sie nicht brauchen. Das Ganze kann natürlich unterstützt werden, indem man

Offensivfähigkeiten bereithält. Mit allen rechtlichen Imponderabilien. Das muss gesetzmäßig verankert sein, sonst kann man nicht offensiv vorgehen. Das erlaubt es dann, wenn mir einer auf den Kopf schlagen will, ihm in die Hand zu fallen. „So geht es nicht mehr!" Und wenn das nicht reicht, vielleicht dem Angreifer auf den Kopf zu schlagen. „Jetzt gibst du aber Ruhe!" Also vom Prinzip her haben Sie vollkommen recht. In die Prävention muss das Schwergewicht der Maßnahmen fließen, weil wir nicht wissen: Kommt eine Attacke? Wie stark kommt sie? Wo setzt sie an? Und weil wir nicht in der Lage sind, vom Militär aus nicht in der Lage sind, alle kritischen Infrastrukturen mit einem Cyberwachbataillon zu schützen. Das wird es nicht geben. Deswegen das NIS-Gesetz (*Netz- und Informationssystemsicherheitsgesetz, Red.*) und die Vorschriften an die Unternehmen, was sie alles an Sicherheit machen müssen.

STATEMENT PUBLIKUM 5

Ich bin ein bisschen erstaunt über diese Diskussion. Sie beschreiben sehr eloquent die Bedrohungen, Sie beschreiben sehr eloquent das Ausmaß der Computerisierung und der Programme. Sie fordern selbstverständlich perfekte Programmiererinnen und Programmierer, die keine Fehler machen. Und selbstverständlich fordern Sie mehr Geld. Aber über das eigentliche Problem haben Sie kein einziges Wort verloren in dieser Diskussion. Was ist das eigentliche Problem? Es ist ein Problem vorhanden, dem man sich stellen muss, und wir bauen Schutzwälle auf. Was aber ist immer – was immer wir auch tun – das schwächste Glied in einem Schutzwall? Der Mensch. Sie haben kein Wort über das Vier-Augen-Prinzip verloren. Über die Möglichkeit, dass ein Abteilungsleiter betrunken ein wichtiges Passwort weitergibt. Menschliche Probleme, menschliches Versagen, das ist das wahre Problem. Und das ist das Problem, das uns beschäftigen wird und das Sie mit noch so schlauen Computertechnikern und perfekten Programmierern niemals lösen werden können.

CARINA KLOIBHOFER

Natürlich wird oft und gern das Synonym verwendet: Der Mensch ist das größte Sicherheitsrisiko. In diesem Zusammenhang sehe ich das aber auch umgekehrt: Der Mensch ist auch das größte Asset, das wir haben. Wir sind immerhin jene, die Systeme weiterentwickeln können. Was nicht außer Acht gelassen werden darf, sind all die organisatorischen Maßnahmen, die getroffen werden müssen. Das heißt, es gibt diverse Trends, man sieht das ebenso in den Budgetaufstellungen, egal ob jetzt staatlich oder organisatorisch. Auf organisatorischer Ebene, also in Institutionen, sieht man einen klaren Trend dahingehend, dass es immer mehr Trainings für alle Anwender- und Anwenderinnengruppen gibt. Das heißt, sei es jetzt für eine normale Abteilung bis hin zu Trainings für ohnehin schon gut geschulte Fachkräfte, etwa in der Systemadministration oder IT-Sicherheit, um diese auch dahin gehend noch spezieller zu schulen. Denn das Problem ist durchaus bekannt und wird mittlerweile wirklich in Angriff genommen mit dem Ziel, diese Schwachstelle des Fehlerpotentials durch Mitarbeiterinnen und Mitarbeiter noch gezielter zu beheben und in eine positive Richtung lenken zu können.

STATEMENT PUBLIKUM 6

Ich bezeichne mich als Blackout-Experten, beschäftige mich seit 2011 mit diesem Thema und danke für das Aufgreifen dieses Themas. Wir reden über das Verhindern. Was ich aber vermisst habe, wir haben keinerlei Antworten gehört zu: Was machen wir, wenn es nicht mehr zu verhindern war? Und wir reden ja nicht nur von Cyberangriffen, die das System zum Kollabieren bringen können, sondern es gibt eine Reihe anderer Möglichkeiten. So wie die Entwicklungen bisher gelaufen sind und in den nächsten fünf Jahren auf europäischer Ebene geplant sind, gehe ich fix davon aus, dass wir diesen Kollaps erleben werden. Und zwar hoffentlich nicht aufgrund eines Cyberangriffes oder durch einen Zwischenfall, wie die Leittechnikstörung 2013, sondern durch Komplexitätsüberlastung. Herr Mandl hat das deutlich angesprochen, die Komplexität steigt massiv an. Und die Frage ist, wie gut wir darauf vorbereitet sind. Und daher möchte ich das Publikum fragen: Wer kann sich und seine Familie zwei Wochen selbst versorgen? Wer kann das?

Damit möchte ich auch die andere Frage, die gestellt wurde, beantworten. Wie lange dauert es? Es gibt Einschätzungen, dass Österreich Vorreiter beim Wiederhochfahren ist. Wenn nicht alles schiefgeht, können wir mit 24 Stunden Stromausfall rechnen, dass es binnen dieser Zeit möglich ist, das wiederherzustellen. Auf europäischer Ebene rechnen wir mit einer Woche.

Das ist aber nicht das Problem. Das Problem ist, dass es dann zumindest mehrere Tage dauert, bis die Telekommunikationsversorgung wieder funktioniert. Und ohne Telekommunikationsversorgung gibt es weder Produktion noch Logistik noch Warenverteilung. Wenn so wenige aufzeigen, die sich zwei Wochen selbst versorgen können, dann haben wir ein Problem, das mit nichts und mit keiner Vorbereitung lösbar ist. Da fängt es bei uns selbst an, genau diese Vorsorge zu treffen, damit hoffentlich die anderen Maßnahmen greifen. Das betrifft ja nicht nur meine Teilnahme hier, sondern ich bin in vielen Organisationen unterwegs. Und das betrifft genauso die Einsatzorganisationen, das betrifft Unternehmen. Wenn die Familie zu Hause ein Problem hat, dann kommen die Menschen nicht, um die Systeme wieder hochzufahren.

RESÜMEE

GEORG BRASSEUR

Mit der Diskussion zu diesem großen, breiten Thema, das heute in nur 90 Minuten abgehandelt wurde, konnte die Problematik nur angerissen und die Wichtigkeit einer ausfallgeschützten Energieversorgung unterstrichen werden. Die Breite des Themas hat auch gezeigt, dass es schwierig sein kann, im Fokus zu bleiben. Noch zur letzten Wortmeldung aus dem Publikum: Es geht weniger um die Versorgung des Einzelnen, sondern um den Ausfall der in hoch industrialisierten Ländern so wichtigen Ressource Strom. Wie können wir als Gemeinschaft darauf reagieren?

Wir haben gehört, dass ein Blackout mit hohem Aufwand verbunden ist, sowohl für den Angreifer als auch für den Verteidiger. Dass es oft auch darum geht, welche Ressourcen beide Seiten zur Verfügung stellen können. Da kann man auch die Frage stellen, ob es nicht manchmal besser wäre, die wichtigsten funktionskritischen Systeme der Elektrizitätsversorgung komplett vom Internet abzukoppeln, weil hohe Mittel in den Schutz dieser Infrastruktur fließen müssen und trotz der hohen eingesetzten Mittel kein vollständiger Schutz, außer durch Abkopplung, erzielt werden kann. Das ändert aber nichts daran, und das ist in der Diskussion klar hervorgetreten, dass wir heute ohne eine vernetzte EDV nichts mehr tun können. Das betrifft sowohl das Betriebssystem, die jeweilige Applikation, aber auch die Hardware, auf der diese Software läuft. Und es wurden auch „Backdoors“ (*eingebauter Zugang zum System unter Umgehung der normalen Zugriffssicherung, Red.*), die man für Cyberangriffe nutzen kann, angesprochen. Da ist man eigentlich ausgeliefert und kann nur hoffen, dass man auf jedem Endgerät grundsätzlich nur selbstgeschriebene Software einsetzt, so wie in der Diskussion mehrfach adressiert, um zumindest dieses Sicherheitsrisiko etwas einzuschränken. Wenn die Software im eigenen Haus entstanden ist, weiß man, ob und wie viele „Backdoors“ eingebaut sind.

Ein weiteres wesentliches Thema ist die ständige Beobachtung der Bedrohung, die ja permanent vorhanden ist, durch Monitoring. Angriffe gehen oft so schnell, so schnell kann ein Mensch gar nicht reagieren. Aber der Mensch kann Systeme erstellen, die dann automatisch und rasch funktionieren, etwa wenn Echtzeitvideos über Facebook oder andere soziale Medien ins Internet gestellt werden. Da hat es Fälle gegeben, ich erinnere an den Massenmord an Jugendlichen durch Anders Behring Breivik, der sein Verbrechen über eine soziale Plattform in Echtzeit ins Internet übertragen hat. Der Massenmord wurde durch die automatische Software relativ spät erkannt und damit auch der Streamingdienst zu spät geblockt. Das heißt, Monitoringsysteme müssten automatisch

und zuverlässig reagieren, um solche Bedrohungsszenarien rechtzeitig zu erkennen und abzudrehen und damit die Intention der Kriminellen – einen Blackout hervorzurufen oder die Welt von ihren (Un)taten zu informieren – zu unterbinden. A la longue muss Software zur Erkennung von Bedrohungsszenarien so treffsicher reagieren wie ein menschlicher Beobachter, nur wesentlich schneller und ohne Ermüdung. Und diese Erkenntnis kann man aus der heutigen Diskussion mitnehmen.

Mir bleibt, mich beim Publikum für das zahlreiche Erscheinen, die Fragen und die Diskussionsbeiträge zu bedanken. Großer Dank geht auch an die Panellisten, an den Leiter der Podiumsdiskussion und an die Mitarbeiterinnen und Mitarbeiter der Akademie, allen voran Frau Weilinger, für die hervorragende Organisation der Veranstaltung.

IMPRESSUM
Herausgeber:
Präsidium der Österreichischen Akademie der Wissenschaften
Dr. Ignaz Seipel-Platz 2, 1010 Wien
www.oeaw.ac.at

Herausgeber des Bandes:
Univ.-Prof. Dr. Georg Brasseur

FOTOS
Cover: © Andrey VP/Shutterstock.com
Seite 7: Foto: ÖAW, Sepp Dreissinger
Seite 9: Foto: Nadja Meister
Seite 10: Foto: AIT
Seite 11: Foto: privat
Seite 12: Foto: privat
Seite 16: Foto: U. Kriebaum

REDAKTION
Mag. Angela Balder

ISBN 978-3-7001-8804-9

ÖAW

WWW.OEAW.AC.AT