


“Alleine können wir es nicht schaffen”

BSI-Präsident Schönbohm fordert Dialogbereitschaft

(BS/th) “Was für Informationen haben wir und wie kann man sie weitergeben?”, fragte Arne Schönbohm, Präsident des Bundesamts für Informationstechnik (BSI), in seiner Eröffnungsrede. Es sei nötig, Informationen zu teilen, um das Sicherheitsniveau zu erhöhen. “Alleine können wir es nicht schaffen”, so der BSI-Präsident.

Als Beleg für seine Aussagen erwähnte *Schönbohm* die zunehmenden Cyber-Angriffe auf Kritische Infrastrukturen in diesem Jahr. “2016 wurden in Deutschland 60 Krankenhäuser durch Ransomware angegriffen.” Der BSI-Präsident machte sich dafür stark, dass Opfer von Erpressertrojanern Anzeige erstatten und kein Geld bezahlen sollten. “Wir raten dazu, kein Lösegeld zu zahlen, weil die Zahlungen das Geschäftsfeld anfeuern.” Das Thema Awareness sei besonders wichtig in Bezug auf Angriffe mit Ransomware, da drei Viertel aller Attacken über infizierte E-Mail-Anhänge erfolgten. Neben der Sensibilisierung der Mitarbeiter sei eine effektive Back-up-Strategie der beste Schutz, um sich gegen Erpressertrojaner zu wappnen.

Bei dem Cyber-Angriff auf das Atomkraftwerk in Grundremmingen habe das BSI laut *Schönbohm* verhindert, dass der Angriff die Steuerung des AKWs erreiche. Im Anschluss sei die gesamte Branche informiert worden, um die eigenen Systeme besser schützen zu können. “Dialog ist nötig, um die Cyber-Sicherheit zu erhöhen”, so *Schönbohm* weiter.

BSI-Präsident Arne Schönbohm wünscht sich einen intensiven Austausch mit der Wirtschaft.

Fotos: BS/Giessen

Um auf das gestiegene Bedrohungspotenzial zu reagieren, hat das Bundesinnenministerium eine “schnelle Eingreiftruppe” für Cyber-Vorfälle gegründet, die beim BSI angesiedelt wird. Sie soll insbesondere Betreibern Kritischer Infrastrukturen nach Angriffen von Cyber-Kriminellen schnell und unbürokratisch helfen. Den “Mobile Incident Response Teams” (MIRT) sollen voraussichtlich 20 Mitarbeiter angehören, die ab 2017 ihre Arbeit aufnehmen werden.

Schönbohm vertrat die Auffassung, dass sich die Rolle seiner Behörde seit der Gründung vor 25 Jahren stark gewandelt habe. “Wir gestalten die Informationssicherheit für Staat, Wirtschaft und Gesellschaft.” In der Anfangszeit sei es dagegen so gewesen, dass ausschließlich die IT-Sicherheit staatlicher Stellen im Fokus des BSI stand.

Der BSI-Präsident hält es für zwingend erforderlich, dass das Thema IT-Sicherheit bei allen Unternehmen auf Vorstandsebene angesiedelt werde. “Es macht keinen Sinn, wenn Vorstände nur über die Chancen der Digitalisierung reden und wenn es um Cyber-Sicherheit geht, heißt es, das mache der ITler.” Er sehe “immer dieselben Gesichter”, wenn er zum Thema IT-Sicherheit spreche.

Für *Schönbohm* ist es elementar, dass ein intensiver Dialog zwischen Wirtschaft und Politik stattfindet. Anders könnte das Niveau der IT-Sicherheit nicht angehoben werden. Das BSI gehe hier mit gutem Beispiel voran. So sei die Frage “Was für Informationen haben wir und wie können wir sie weitergeben?” eine der Leitlinien seiner Behörde.

“Es boomt in allen Geschäftsfeldern”

Der Vizepräsident des BfV zur Arbeit des Verfassungsschutzes

(BS/th) Über mangelnde Arbeit kann sich das Bundesamt für Verfassungsschutz (BfV) nicht beklagen, wie Vizepräsident Thomas Haldenwang in seinem Vortrag erläuterte. “Es kehrt nie Ruhe ein”, sagte er mit Blick auf Themenfelder wie den islamistischen Terrorismus oder den Bereich Cybercrime.

Haldenwang äußerte den Wunsch, dass nicht nur die Chancen, sondern auch die Risiken der Digitalisierung stärker beachtet werden müssten. “Technologischer Fortschritt wird oft nur positiv betrachtet, obwohl es auch Schattenseiten gibt. Es boomt in allen Geschäftsfeldern”, so *Haldenwang* zur Arbeit des Inlandsgeheimdienstes. “Das Netz ist auch ein Raum der Unsicherheit.”

Haldenwang machte sich für eine stärkere Zusammenarbeit mit der Wirtschaft stark. “In diesem Zusammenhang ist besonders die Initiative Wirtschaftsschutz zu nennen.” Der Plattform gehören neben dem BfV unter anderem das Bundesamt für Sicherheit in der Informationstechnik, das Bundeskriminalamt, der Bundesnachrichtendienst und der Bundesverband deutscher Industrie e. V. an, um sich über Cyber-Sicherheit auszutauschen.

Die zunehmende Professionalisierung von Cyber-Kriminellen zeigt sich für *Haldenwang* auch darin, dass Angriffe aus

Thomas Haldenwang sprach u.a. über Wirtschaftsspionage.

Ländern gestartet werden können, die nicht einmal über eine ausreichende IT-Infrastruktur verfügten. Als Beispiel nannte er hier den Angriff auf den Elektronikkonzern Sony, der mutmaßlich durch Nordkorea durchgeführt wurde, um die Ausstrahlung des Films “The Interview” zu verhindern, in dem Diktator *Kim Jong Un* persifliert wird. “Die Effizienz von Angriffen ist im Cyberraum eine ganz andere”, so *Haldenwang*. Als wichtiges Aufgabenfeld sprach der BfV-Vize auch das Thema Spionageabwehr an. Hier habe der Inlandsgeheimdienst zwar schon immer einen 360-Grad-Blick gehabt, jedoch liege der Schwerpunkt in diesem Bereich aus einem sehr naheliegenden Grund auf Ländern wie China und Russland. “Dort sind die Dienste vom Gesetzgeber verpflichtet, an dem technologischen Fortschritt des Landes mitzuarbeiten.” Der Staat beauftrage die Dienste somit mit Wirtschaftsspionage.

Haldenwang appellierte an die Unternehmen, sich bewusst zu machen, was die wertvollsten Daten seien, damit hierauf die IT-Sicherheitsstrategie aufbauen könne. “Kronjuwelen müssen gesondert geschützt werden”, so *Haldenwang*. Auch müsste sich jeder im Klaren darüber sein, dass die zunehmende Vernetzung das Risiko für erfolgreiche Cyber-Attacken noch erhöhe. “Mobile Endgeräte sind ein Einfallstor für Angriffe.”

“Cyber-Angriffe sind wie Radioaktivität”

IT-Sicherheit im Hochtechnologiebereich

(BS/th) Für Hans-Joachim Popp sind besonders Unternehmen im Hochtechnologiebereich anfällig für Wirtschaftsspionage. “Unser Know-how ist für andere von Interesse”, so der CIO des Deutschen Zentrums für Luft- und Raumfahrt.

Als Beispiel für Geschäftsgeheimnisse, an denen auch andere Unternehmen Interesse haben könnten, führte er die kartografische Vermessung der Erde aus dem All an, die das Deutsche Zentrum für Luft- und Raumfahrt unter großem Aufwand durchgeführt habe.

Um Unternehmen und Institutionen besser schützen zu können, sieht *Popp* besonders den Staat in der Pflicht. “Cyber-Attacken sind wie Radioaktivität. Wir haben gelernt, damit zu leben”, so der CIO. Er machte sich in seinem Vortrag dafür stark, das Internet stärker zu regulieren. Dies könne unter anderem dadurch geschehen, dass man verhindere, dass Cyber-Kriminelle mit Schadsoftware hinterlegte Webseiten bauen würden, die seriös klingende Namen haben. “Der Wilde Westen im Cyber-Raum ist völlig ohne Regulierung.” Dies könne mittelfristig aus Sicherheitsgründen nicht so bleiben.

Um sich vor Angriffen möglichst gut zu schützen, sei es unerlässlich, dass Unternehmen und Staat eng miteinander zusammenarbeiteten und ihr Wissen teilten. Die zunehmende Vernetzung mache es zudem unerlässlich, dass die Nutzung sämtlicher IT durch die Unternehmen kontrolliert wird. Dies gelte insbesondere dann, wenn die Mitarbeiter ihre privaten Endgeräte beruflich nutzen würden. “Unsere IT hat vollen Zugriff auf die privaten Geräte, die für dienstliche Zwecke genutzt werden. Anders geht es nicht”, so *Popp*.

Hans-Joachim Popp wünscht sich mehr Regulierung durch den Staat.

Handlungsoptionen für mehr IT-Sicherheit

Der CIO gab den Teilnehmern des Münchner Cyber Dialogs konkrete Handlungsoptionen mit auf den Weg, um das Sicherheitsniveau zu erhöhen. “Man sollte sich fragen, welche Systeme mit dem Internet verbunden sein müssen.” Insbesondere Back-ups sollten offline aufbewahrt werden. “Wichtig ist auch, das Need-to-know-Prinzip umzusetzen”, so *Popp,* der mit der Aussage darauf abzielte, dass die Kontrolle von Zugriffsrechten ein Mittel sein, um das Sicherheitsniveau zu erhöhen und so zu verhindern, dass Cyber-Attacken über einzelne Computer gesamte Systeme infiltrieren könnten. “Nichts zu tun und die Systeme einfach laufen zu lassen, ist keine Option.”

Die Rolle des Staates stärken

Staatssekretär und Verbandschef für mehr Engagement

(BS/th) “Wenn die öffentliche Verwaltung will, kann sie sehr schnell arbeiten”, so Dr. Michael Wilhelm, CIO des Freistaates Sachsen. Diese hohe Leistungsfähigkeit könne man sich zunutze machen, wenn es darum geht, die IT-Sicherheit in Deutschland zu erhöhen. Hierzu seien aber größere Anstrengungen hinsichtlich der Standardisierung nötig.

“Es müssen Vereinheitlichungen her”, so der Landes-CIO. Er erwarte, dass die Bürger nur ein einziges Nutzerkonto benötigen, um Angebote zum E-Government wahrzunehmen. Der IT-Planungsrat arbeite hier an einer Lösung.

Die Notwendigkeit, für ein hohes Sicherheitslevel zu sorgen, machte *Wilhelm* mit einer Zahl deutlich. “Wir haben in Sachsen allein im April rund 10.000 verschiedene Trojaner aufgespürt”, würdigte der Landes-CIO die Arbeit des Cybercrime-Kompetenzzentrums des sächsischen Landeskriminalamts. *Wilhelm* machte deutlich, dass die Zahl der tatsächlichen Schadprogramme noch deutlich höher liege. “Es gibt eine hohe Dunkelziffer bei Meldungen von Cyber-Angriffen.”


Dr. Michael Wilhelm und Dr. Klaus Mittelbach waren sich darin einig, dass die Politik die Rahmenbedingungen hinsichtlich der IT-Sicherheit setzen muss.

Stärkere Beachtung der Industrie gefordert

“IT-Sicherheit ist nur eine Seite der Medaille Cyber-Sicherheit”, so *Dr. Klaus Mittelbach,* Vorsitzender der Geschäftsführung des Zentralverbands Elektrotechnik- und Elektroindustrie e. V. (ZVEI). Die andere Seite ist für ihn die “Industrial Security”. “Die Industrie 4.0 ist für uns von überragender Bedeutung.” Trotzdem werde den speziellen Bedürfnissen der IT-Sicherheit in diesem Bereich oftmals eine zu geringe Bedeutung beigemessen. Hier nannte er u. a. die Geschwindigkeit, mit der heutzutage Produktionen ablaufen würden. “Wir arbeiten zunehmend in Echtzeit. Dies ist in der IT nicht der Fall”, so *Mittelbach.*

Er misst der Elektroindustrie eine Schlüsselrolle beim Gelingen der Modernisierungen im Rahmen der Industrie 4.0 zu. “Wir besitzen schon lange eine hohe Kompetenz für Software in der Maschine”, so der Verbandschef, der die Politik in der Pflicht sieht, einheitliche Sicherheitsstandards zu schaffen. “Wichtig ist, dass wir das Thema Cyber-Sicherheit in Europa organisiert bekommen.” Die IT-Sicherheit ist für *Mittelbach* ein entscheidender Faktor für die Zukunftsfähigkeit des Standorts Deutschland.