Außerordentliche Bedrohungslage fordert Umdenken in der IT-Sicherheit

Bundesregierung und EU reagieren mit strengen Verordnungen und drakonischen Strafen

IT-Sicherheit bestimmt die Schlagzeilen, weil sich drastische Fälle häufen. Experten beobachten die rasant steigende Zunahme schädlicher Programme mit großer Sorge: So werden täglich unglaubliche 400.000 neue Varianten von Schadprogrammen entdeckt. Der prominenteste Vertreter dieser Spezies dürfte die »WannaCry«-Schadsoftware sein, die sich Mitte Mai mit rasanter Geschwindigkeit verbreitete – Experten geben hier dem amerikanischen Geheimdienst NSA eine Mitschuld, da sie die Lücke in der Software nicht an Microsoft gemeldet haben [1].

Mit »WannaCry« nehmen die Angriffe eine neue Dimension an: »Wenn informationstechnische Systeme von Unternehmen, Krankenhäusern oder Verwaltungen lahmgelegt werden, um ›Lösegeld‹ zu erpressen, ist das eine Entwicklung, die ein entschiedenes Handeln erfordert«, äußerte der Bundesinnenminister de Maizière [2]. IT-Sicherheit muss sich in diesen Tagen neu erfinden und wird auch zum Politikum.

Anlässlich eines Symposiums der AXSOS AG aus Stuttgart sprach »der berühmteste Virenjäger Europas«, Mikko Hypponen, Chief Research Officer von F-Secure, bereits 2015 über die Rolle von Regierungen und dem Schutz vor Cyberattacken. So nennt Hypponen WannaCry jetzt »den größten Ransomware-Ausbruch in der Geschichte« [3].

Die Politik setzt die IT-Sicherheit mit Priorität auf die Agenda. Dass die Politik Handlungsbedarf sieht, wird allein in zwei Neuerungen deutlich: dem IT-Sicherheitsgesetz in Deutschland sowie der Europäischen Datenschutzgrundverordnung. So brachte die Bundesregierung bereits 2015 das IT-Sicherheitsgesetz auf den Weg, in dem Unternehmen verpflichtet wurden, Hackerangriffe an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das Gesetz umfasst insbesondere Unternehmen der kritischen Infrastrukturen. In einem zweiten Schritt soll die Meldepflicht allerdings ausgeweitet werden. Wer dieser Meldepflicht nicht nachkommt, den erwartet eine Strafe in sechsstelliger Höhe.

Der »berühmteste Virenjäger Europas«, Mikko Hypponen (links), Chief Research Officer von F-Secure bezeichnet WannaCry als »den größten Ransomware-Ausbruch in der Geschichte«. Rechts Frank Müller, Vorstand der AXSOS AG.

Endlich einheitlicher Datenschutz für Europa. Die politische Verantwortung wurde erkannt und zieht mit der Europäischen Datenschutzgrundverordnung (EU-DSGVO) globalere Konsequenzen nach sich. Mit der neuen Verordnung werden einheitliche Regeln für einen besseren Datenschutz in der digitalen Arbeitswelt umgesetzt.

Bußgelder in Millionenhöhe drohen, bei Unternehmen jeder Größenordnung. Der Datenschutz soll in der gesamten EU harmonisiert werden, allerdings werden davon auch außereuropäische Unternehmen betroffen sein: Besonders Firmen, die Waren oder Dienstleistungen in der EU anbieten und somit Einfluss auf die Verarbeitung personenbezogener Daten von Bürgern der EU haben. Im Gegensatz zum IT-Sicherheitsgesetz sind hier die Bußgelder in empfindlicheren Regionen angesetzt, so können bei Nichteinhaltung vier Prozent des jährlichen, weltweiten Umsatzes des Unternehmens oder 20 Millionen Euro erreichen – je nachdem, welcher Wert höher ist.

Unternehmen dürfen keine Zeit verlieren. Die EU-Datenschutzgrundverordnung gilt ab dem 25. Mai 2018, ein Termin der seit längerem bekannt ist, sodass man sich entsprechend vorbereiten konnte. Falls noch nichts unternommen wurde, sollte jetzt umgehend damit begonnen werden, denn die Umsetzung aller Kernpunkte nimmt relativ viel Zeit in Anspruch.

Eva Wachter

[1] http://www.zeit.de/digital/datenschutz/2017-05/wannacry-ransomware-attacke-hackerangriff-it-deutsche-bahn/komplettansicht

[2] https://www.tagesschau.de/inland/cyberangriffe-107.html

[3] http://www.zeit.de/digital/datenschutz/2017-05/wannacry-ransomware-attacke-hackerangriff-it-deutsche-bahn/komplettansicht

Experteninterview

»IT-Sicherheit beginnt beim Mitarbeiter«

Experten im Gespräch: Peter Klien (links) und Bernd Länge (rechts).

Wie schätzen Sie die Bedrohungslage in Deutschland ein, gerade auch im Hinblick auf die aktuellen Attacken?

Bernd Länge: Deutschland war und ist ein Hightech-Standort, das macht uns zum gern genommenen Ziel von Industriespionage und ganz gezielten Attacken. Der Schaden, der hier in der Vergangenheit für betroffene Unternehmen entstand, war immens und hat sich nicht nur in Kosten niedergeschlagen, sondern bedeutet auch nicht zu reparierende Schäden im Image und vor allem auch im Wissen, das für immer verloren gegangen ist.

Peter Klien: Was wir auch feststellen können, ist, dass sich die Angriffe in ihrer Art verändert haben. Das haben wir jetzt mit WannaCry erfahren. Früher waren es Malware-Angriffe, die Schwachstellen von Unternehmen ausgenutzt haben, heute erleben wir zielgerichtete und wesentlich effektivere Angriffe. Und zwar nicht ausschließlich auf die großen Unternehmen, sondern vornehmlich auf das Know-how des innovativen, deutschen Mittelstands.

Wie sicher ist die IT in deutschen Unternehmen?

Bernd Länge: Die meisten Unternehmen, die ich kenne, haben ein akzeptables Schutzniveau etabliert. Das bedeutet aber nicht, dass man sich hier beruhigt zurücklehnen kann – im Gegenteil: Je nach gesetzlicher Anforderung, oder teilweise auch bedingt durch Anforderungen als Lieferant, müssen manche Unternehmen im IT-Sicherheitsbereich massiv aufrüsten.

Peter Klien: Bedenklich ist, dass die Unternehmen einen Angriff an sich in den meisten Fällen gar nicht bemerken, sondern irgendwann feststellen müssen, dass Daten abfließen. Schutzmechanismen, die ein solches Eindringen verhindern, sind in jedem Fall aufzubauen.

Sind die Verordnungen der Politik hilfreich beziehungsweise nutzen Gesetze wie das IT-Sicherheitsgesetz oder die EU-Datenschutzgrundverordnung überhaupt etwas?

Bernd Länge: Gesetze beziehungsweise die neue EU-Datenschutzrichtlinie ist auf jeden Fall sinnvoll. Sie zwingt Unternehmen, die noch keinen adäquaten Schutz haben, nachzubessern und das mit harten Maßnahmen: So haftet der CEO und der IT-Leiter auch mit seinem Privatvermögen. Das zeigt den Stellenwert von IT-Sicherheit: Ein guter Schutz hilft am Ende eben allen.

Peter Klien: Meiner Meinung nach ist es hier besonders wichtig, auch die Mitarbeiter entsprechend zu sensibilisieren. Das beste Gesetz bringt nichts, wenn die Mitarbeiter nicht wissen, was das für sie konkret bedeutet. Das sollte man bei der Umsetzung dieser Gesetze immer im Hinterkopf behalten.

Bernd Länge ist seit über 15 Jahren in der IT-Branche tätig. Seit 2014 ist er Bereichsleiter Infrastruktur und Security der AXSOS AG aus Stuttgart.

Tel. 0711 / 901196 441
bernd.laenge@axsos.de

Peter Klien ist seit über 17 Jahren in der IT-Security-Branche tätig. Seit 2017 arbeitet er als Account Manager im Bereich Infrastruktur und Sicherheit für die AXSOS AG aus Stuttgart.

Tel. 0711 / 901196 444
peter.klien@axsos.de