Kaspersky Lab (KL)-Experten Ekaterina Rudina, Senior Analyst System Security. (links) und Andrey Suvorov, Director of Critical Infrastructure Protection (rechts)

Eine Frage der nationalen Sicherheit:

Wie Russland seine kritischen Infrastrukturen vor Cyberangriffen schützen will

Deutschland gab sich schon 2015 ein IT-Sicherheitsgesetz. Ein Jahr später verabschiedete die EU die Netz- und Informationssicherheits-Richtlinie (NIS). Russland zog erst 2017 Konsequenzen aus der neuen Bedrohungslage. Über das neue Informationssicherheitsgesetz, die Cyberimmunität kritischer Infrastrukturen und sichere Technologien sprach B&D mit Kaspersky Lab (KL)-Experten Andrey Suvorov, Director of Critical Infrastructure Protection, und Ekaterina Rudina, Senior Analyst System Security.

DIGITALE TRANSFORMATION GELINGT NUR MIT IT-SICHERHEIT. DAS HABEN DIE JÜNGSTEN, GLOBAL ANGELEGTEN CYBERATTACKEN DEUTLICH GEZEIGT. WARUM HAT RUSSLAND SO SPÄT DIE BEDEUTUNG DES SCHUTZES KRITISCHER INFRASTRUKTUREN ERKANNT UND ERST AM 26. JULI 2017 EIN ENTSPRECHENDES GESETZ BESCHLOSSEN?

Das lag an der Staatsduma, die lange über den Entwurf beriet. Es ist nicht ausgeschlossen, dass die Abgeordneten statt eiliger Beschlüsse zuerst die internationale Praxis studieren wollten. Die Endfassung unterscheidet sich sehr von der ursprünglichen, sie ist professioneller und lässt weniger Umgehungsmöglichkeiten zu.

WAS ÄNDERT SICH MIT JAHRESBEGINN FÜR DIE BETREIBER KRITISCHER INFRASTRUKTUREN (KRITIS) IN RUSSLAND, WENN DAS GESETZ IN KRAFT TRITT?

Die Änderungen werden sich erst mit der Zeit einstellen. Das Gesetz legt nur den Rahmen fest. Aktuell führt die Regierung Konsultationen über die Relevanzkriterien durch, danach wird sie eine Einteilung von KRITIS-Objekten nach Relevanz vornehmen und ein Register aufsetzen. Unternehmen aus diesem Register werden als relevante kritische

Infrastrukturen eine Reihe von Sicherheitsmaßnahmen implementieren müssen. Dazu gehört auch die Verbindung mit dem GosSOPKA-System (russisch: ГосСОПКА), das nationale Informationssicherheits-System in Verantwortung des Cybersicherheitsorgans, das das IT-Lage-Monitoring und im Krisenfall die Koordination übernimmt.

WIE IST DEUTSCHLAND IHRER MEINUNG NACH IM BEREICH IT-SICHERHEIT AUFGESTELLT?

Wir verfolgen Regulierungsansätze verschiedener Länder. Was die Absicherung der KRITIS anbelangt, ist Deutschland nicht nur Russland, sondern auch vielen anderen Ländern voraus. Der deutsche Ansatz im Bereich Cybersicherheit ist ausgereift und für viele Länder eine Benchmark, die es zu adaptieren und gemäß nationaler Prioritäten weiterzuentwickeln gilt.

DIE AUSWAHL DER KRITIS-BRANCHEN, IST ZENTRAL FÜR DEN AUFBAU DER NATIONALEN CYBERSICHERHEITS-ARCHITEKTUR. HAT DER RUSSISCHE GESETZGEBER HIER EINE KLUGE AUSWAHL GETROFFEN?

Laut Gesetz zählen in erster Linie Staatsorgane und Verwaltung, Industrie, Öl-, Gas- und Energiewirtschaft, Transport, Telekommunikation, Banken- und Gesundheitswesen zu kritischen Infrastrukturen. Ob das klug gewählt ist, kann man nicht eindeutig sagen. Wir würden nicht zu kleinteilig vorgehen. Zudem zeigt die internationale Praxis, dass der KRITIS-Schutz am effektivsten ist, wenn er allgemeine Vorschriften und branchenspezifische Standards kombiniert. Bei Branchenanforderungen sollten die Aufseher in jedem Fall Vertreter von Industrie- und Technologieunternehmen konsultieren – und den Austausch fortführen, beispielsweise als Public Private Partnership – so vermeidet man manche unsinnige Regelung. Unter diesen Gesichtspunkten wirkt das russische Gesetz sehr professionell, es lässt Freiraum für einen solchen Austausch.

WELCHE ROLLE SPIELEN IN RUSSLAND DIE CERTS (COMPUTER EMERGENCY RESPONSE TEAM), ALSO IT-KRISEN-REAKTIONSZENTREN?

Es gibt bereits mehrere private und staatliche CERTs in Russland. Auch KL hat seit 2016 ein eigenes KL ICS (Industrial Control Systems) CERT. Seine Aufgabe ist, Aktivitäten von Herstellern industrieller Steuerungssysteme, Betreibern und IT-Sicherheitsforschern weltweit zu koordinieren. Es pflegt auch Verbindungen zu Regulierungsbehörden und Notfallzentren in anderen Ländern wie zum US ICS-CERT in den USA und JPCERT/CC in Japan. Denn die Cyberabwehr ist effektiv nur im Verbund.

BEHINDERN AKTUELLE SPANNUNGEN ZWISCHEN EINZELNEN LÄNDERN NICHT DIE INTERNATIONALE KOOPERATION?

Grundsätzlich steht einer Kooperation nichts im Wege. Schon heute läuft der Informationsaustausch über Cyberrisiken und Sicherheitslücken in der Regel reibungslos – auch im Rahmen der FIRST-Assoziation (Forum of Incident Response and Security Teams), zum Beispiel mit Japan und Australien.

GIBT ES KOOPERATIONSBEISPIELE ÜBER CERT-VERBÜNDE HINAUS?

Nehmen Sie die Cyberkriminalität. Aufklärung und Prävention von Cyberstraftaten wären ohne Mitwirkung von Sicherheitsexperten undenkbar. Kaspersky Lab arbeitet seit 2014 in kriminalpolizeilichen Angelegenheiten mit Interpol zusammen. Wir sind bereit, auch mit Europol enger zu kooperieren. Es gibt bereits ein Memorandum, unterzeichnet von unserem CEO Eugene Kaspersky und Troels Oerting, dem Chef des European Cybercrime Centre (EC3).

WIE SOLLEN WIR UNS IHRE ZUSAMMENARBEIT MIT INTERNATIONALEN STRAFVERFOLGUNGSBEHÖRDEN KONKRET VORSTELLEN?

Als Interpol 2017 ein Netz aus infizierten Servern in Südostasien sowie Hunderter kompromittierter Webseiten, darunter Regierungsportale der ASEAN-Länder, aufgedeckt hat, waren unsere Experten an dieser Operation beteiligt. 2015 nahm KL an einer Aktion des Interpol Global Complex for Innovation (IGCI) teil, um das weltweit operierende Botnetz Simda aus mehr als 770.000 gekaperten Computern zu Fall zu bringen. Die gemeinsame Cyberabwehr ist wichtig – und doch greift sie allein zu kurz. Was wir brauchen, ist eine neue Qualität von vernetzten Systemen in Bezug auf die Cybersicherheit.

IST ES DAS, WAS EUGENE KASPERSKY „CYBERIMMUNITÄT DER KRITISCHEN INFRASTRUKTUREN" NENNT?

Nur wenn sich automatisierte Steuerungssysteme oder das industrielle Internet-of-Things von vornherein auf einem sicheren Fundament aufbauen, sind sie wirklich resilient gegen Hackerattacken. „Fundament" meint IT-Sicherheitsstandards und sichere Plattformen mit eingebauter Cybertechnologie. Bislang gibt es dafür kein Prüfsiegel. Deshalb sind wir froh über die fruchtbare Zusammenarbeit mit den führenden Fachvereinigungen wie dem Industrial Internet Consortium, dem Institute of Electrical and Electronics Engineers (IEEE), der Internationalen Fernmeldeunion oder der OPC Foundation. Die Optionen der Zusammenarbeit sind vielfältig. Und sie beschränken sich nicht auf Expertengemeinschaften. Cybersicherheit ist auch für die UNIDO (United Nations Industrial Development Organization) ein Kernthema.

Es braucht Zeit, bis Resultate dieser fundamentalen Arbeit sichtbar werden. Doch der Zugewinn an Informationssicherheit wird umso nachhaltiger sein.

Das Gespräch führte und übersetzte Svetlana Alexeeva, Strategieberaterin & Autorin für Digitaltransformation und Internetregulierung

DIPL.-KFFR. DIPL.-PHIL.
SVETLANA ALEXEEVA

ist Expertin für Digitaltransformation & Internetpolitik sowie Business Advisor (Russland/GUS)

DIGITAL INSIGHT:
Svetlana.Alexeeva@digital-insight.de

Fotos: Kaspersky Lab