2. DEUTOR Cyber Best Practices Conference, 05.12.2019, Saarbrücken

Herausforderungen für die internationale Cybersecurity

(Challenges for the international Cybersecurity)

Oberstleutnant Franz Lantenhammer, NATO CCDCOE, Tallinn (11:30 – 11:50)

Die technologischen Entwicklungen unserer Zeit sorgen für eine große Dynamik, die Staat, Wirtschaft, Gesellschaft und jeden Einzelnen gleichermaßen erfasst.

Staat, Gesellschaft und Wirtschaft sind von einer funktionierenden und vor allem sicheren IT-Infrastruktur und verlässlichen Informationsversorgung abhängig. Informationstechnik durchdringt unser tägliches Leben, der Grad der Digitalisierung in unserer Gesellschaft steigt unaufhörlich.

Die Herausforderung ist, mit dieser Dynamik Schritt zu halten, damit sie in geordneten Bahnen sicher abläuft und allen Zielgruppen größtmöglichen Nutzen bringen kann. [BSI]

Gleichzeitig erleben wir, dass täglich neue Schwachstellen in Software, Hardware und Konfiguration entdeckt werden. IT-

Sicherheitsvorfälle werden nicht mehr nur in den Fachmedien regelmäßig diskutiert. Alleine in den ersten 3 Quartalen 2019 wurden über 12.000 neue Schwachstellen in IT-Produkten in der Common Vulnerability Database (CVE) aufgenommen (QUELLE/LINK).

Angriffe auf die Informationssysteme werden von der Bevölkerung und den Unternehmen als eine der größten Bedrohungen wahrgenommen. In Umfragen und Untersuchungen rangieren diese regelmäßig unter den TOP 3 bis TOP 5 in den Ranglisten.

Wie das BSI in seinem kürzlich veröffentlichtem Bericht zur Lage der IT-Sicherheit in Deutschland 2019 feststellt, ist die Gefährdungslage in der IT-Sicherheit unverändert hoch und die Bedrohung der Nutzer durch Schadsoftware, Ransomware, Botnetze oder DDoS nimmt weiter zu. Ein besonderes Augenmerk ist auf kritische Infrastrukturen zu richten. Im Berichtszeitraum des Lageberichts wurden dem BSI 252 Vorfälle von Betreibern kritischer Infrastruktur gemeldet.
[BSI, Die Lage der IT-Sicherheit in Deutschland 2019, Oktober 2019]

Wer sind die Akteure:

In vielen Fällen handelt es sich um Kriminelle, oft auch aus dem Bereich der organisierten Kriminalität. Darüber hinaus haben wir es aber auch häufig mit staatlichen Akteuren zu tun, beziehungsweise mit Akteuren, die staatlich geduldet und unterstützt werden. Immer wieder kann man feststellen, dass die Angreifer auch aus verschiedenen Gruppen zusammengesetzt sind, wobei es dann zu einer unklaren Gemengelage kommt, bei der kriminelle Kräfte von Staaten für eigene Zwecke, so zum Beispiel für Spionage, Datendiebstahl, Informationsnmanipulation und sogear für militärische Computernetzwerkoperationen angeheuert werden. Die Professionalität der Täter und Gruppierungen nimmt stetig zu.

Die scheinbare Grenzenlosigkeit des „world wide web“ und der Informationstechnologie führt zu einer Veränderung der Beteiligten und der Verantwortlichen. Informationssyteme sind durch ihre Interkonnektivität von überall erreichbar. Und jedes System mit einem Interface kann Ziel eines Angriff sein. Um Daten auszuspähen, zu zerstören oder Systeme zu manipulieren. Gewollt oder als kollaterales Ziel.

Computer Security Incidents sind nicht mehr nur technische Vorfälle, die durch CERT-s oder Rapid Response Teams gelöst werden können. Angriffe auf Informationssysteme sind immer häufiger auch politisch motiviert und stellen die nationale Souveränität auf die Probe, auf die auch mit politischen Mitteln reagiert werden muss.

Inwieweit Angriffe auf Informations- und Telekommunikationstechnologie die gesamte Gesellschaft betreffen können, kann man am Beispiel von NotPetya betrachten. Ich will hier gar nicht auf die technischen Einzelheiten der Schadsofware und des Angriffs eingehen. Dazu gibt es reichlich Lesestoff und Analysen.
Das Bemerkenswerte bei NonPetya ist seine rapide Ausbreitung über Länder- und Unternehmensgrenzen hinweg. Innerhalb von Stunden wurden IT-Systeme zu wertlosem Blech. Dadurch wurden Organisationen und Unternehmen aus den Bereichen Finanzwirtschaft, Transport, Energie, Handel und der Gesundheitssektor außer Gefecht gesetzt. Zehntausende Maschinen wurden weltweit in kürzester Zeit infiziert. Man spricht sogar von der heimtückischsten viralen Infektion seit der Spanischen Grippe von 1918.

Non Petya war dabei nicht finanziell motiviert, die Angreifer haben die Schadsoftware lediglich als Ransomware getarnt. In Realität hat NonPetya dazu geführt, ganze Netzwerke unbrauchbar zu machen. Der geschätzte Schaden übersteigt 10 Milliarden US Dollar, wobei die immateriellen Kosten gar nicht berücksichtigt sind. Letztlich ist im Falle von NotPetya die Höhe des Schadens entscheidend, sondern die Auswirkung auf die globale Wirtschaft und deren politische Bedeutung.
[Cyber Peace Institute]

IT-Systeme sind eben auch kein Selbstzweck. Sie dienen letztlich immer einem Geschäftsprozess, einem Betriebsablauf oder einer Operation als Antrieb oder Werkzeug. Da aber eben immer mehr Prozesse durch Informationssysteme unterstützt und gesteuert werden, werden sie zum Kern der Betrachtung. Dies ist vor allem im Zusammenhang mit der Steuerung von kritischer Infrastruktur der Fall.

Gegnerische Kräfte und Staaten suchen mittels Angriffen auf Informationssysteme und Internetressourcen aber auch geopolitische Vorteile zu erlangen. Dazu zählt auch die Einflussnahme mit Mitteln des Internet und der Informationstechnik, vor allem mit Hilfe von Sozialen Medien.

Dabei ist die Beeinflussung von demokratischen Prozessen und Wahlen durch ausländische Kräfte äußerst besorgniserregend. Die U.S. Wahlen 2016 waren hier ein deutliches Beispiel.

Neue Technologien bringen auch immer neue Herausforderungen mit sich. Bei der Einführung von neuen Technologien stellt sich daher für mich immer die Frage, was ist der Nutzen und welche Risiken handelt man sich ein. Risikomanagement mit den Schritten „Identifizieren (identify), Schützen (protect), Entdecken (detect), Verteidigen (defned) und Wiederherstellen (recover) hilft dabei die strategische Autonomie zu stärken.

Ein klassisches Beispiel ist die aktuelle Diskussion um die Einführung des 5G Standards und mit welchen Partnern man dabei vertrauensvoll zusammenarbeiten kann. Dabei sind sowohl wirtschaftliche Aspekte aber vor allem auch Sicherheitsfragen zu betrachten. Eine klare Strategie und Zielsetzung von politischer Seite ist dabei die unbedingte Voraussetzung.

Nationen und Organisationen haben in den vergangenen Jahren verstärkt an der Erstellung und Einführung von Cyber Security Strategien gearbeitet. Hier kann man auch den Trend feststellen, dass diese Strategien weg vom Ansatz „Schutz von

Systemen“ zum Risikomanagement und Resilienz Gedanken getrieben werden. Dieses fußt auf einer szenario-basierten Risikobewertung, wobei die Schwere und die Wahrscheinlichkeit eines Risikos sowie die eigenen und gegnerischen Fähigkeiten analysiert werden, ein Plan zum Schutz der Systeme erarbeitet wird, sowie Maßnahmen zur Reaktion auf krisenhafte Situationen vorbereitet werden.

Dabei gehen die Nationen unterschiedliche Wege:
Zum einen gibt es den Ansatz, das Notfallmanagement im Falle eines Cyberangriffes in ein allgemeines Krisenmanagementsystem zu integrieren. Beispiele dafür finden wir in Estland und den Niederlanden.
Der andere Ansatz ist, Cyberangriffe als eingeschränkten (limited) Notfallstatus anzuerkennen, sozusagen „Cybernotfall“. Ein Verteter für diese Betrachtungsweise ist die Tschechische Republik.

Wie unterscheiden sich diese Strategien im Einzelnen?
In der estnischen Strategie werden die Rollen und Verantwortungen für den Normalzustand und den Krisenfall nicht verändert. Die Information Systems Agency (RIA) ist die zentrale Ansprechstelle für den Betrieb aber auch die Reaktion auf IT-

Sicherheitsvorfälle bis hin zum Krisenfall. Der durch das Kabinett beschlossene Notfallpla legt Koordination und Funktionen fest. Dies schließt die Führungsrolle und die Stabsfunktion der RIA und anderer Organisationen sowie Kontinuität der Dienstleistungen und der öffentlichen Kommunikation ein. Die Rollen und Verfahren werden regelmäßig bei Übungen überprüft (und mussten bereits ein Mal in der Realität umgesetzt werden).

Beim tschechischen Cyber Security Act von 2015 wird der begrenzte Krisenfall, bekannt als „state of cybe emergency“ als Handlungsgrundlage festgelegt. Diese begrenzte Cyberkrise kann erklärt werden, wenn die nationalen Interessen in großem Maßstab in Gefahr sind. Die Entscheidung darüber trifft der Direktor der Nationalen Cyber and Information Security Agency (NCISA). Die NCISA kann daraufhin die Betreiber von Informations- und Telekommunikationssystemen verpflichten, bestimmte Cyberssicherheitsmaßnahmen umzusetzen. Nationale Übungen mit technischen und strategischen Szenarien überprüfen regelmäßig die Wirksamkeit der Verfahren. Sie sind thematisch orientiert und beziehen jedes Jahr andere Wirtschafts- und Industriesektoren mit ein.

Strategische Cyber-Übungen sind ein wichtiger Mechanismus, um nationale Prozesse und Verfahren zu überprüfen und zu vertiefen, die in den nationalen strategischen Vorgaben und der Gesetzgebung verankert sind. Übungen vertiefen die Praxis und Erfahrungen der „whole-of-society/whole-of-government“ Koordination bei der Reaktion auf IT-Sicherheitsvorfälle und Cyberoperationen. Für Entscheider auf strategischer Ebene ist es wichtig zu verstehen, welche Auswirkungen Computer Security Incidents auf nationale kritische Infrastrukturen haben und welche Folgen die Reaktion auf solche Vorfälle bewirken kann. Die Übung Locked Shields des NATO Cooperative Cyber Defence Centre of Excellence ist eine excellente Möglichkeit für u sere Mitgliedsnationen gemeinsam mit Partnern diese Prozesse zu prüfen und der Wirksamkeit zu testen. Dabei kann zum Beispiel festgestellt werden, obLücken oder Inkonsistenzen in der Gesetzgebung bestehen, die Verfahren zum Austausch von Informationen wie gewollt funktionieren und ob die Aufgaben und die Verantwortung richtig verteilt sind. Gibt es einen Single point of contact, der die Reaktion und das Incident Response zwischen öffentlicher Verwaltung und Privatwirtschaft oder zwischen zivilen und militärischen Stellen koordiniert?

Diese Aspekte können gesamtstaatlich beim strategischen Anteil der Locked Shields Übung geübt werden. Die Übung ist darauf ausgelegt, nationale Besonderheiten zu berücksichtigen.

- Insgesamt kann man feststellen, dass die spezifische Aufstellung weniger wichtig ist, als die Kompetenzen, Fähigkeiten, Anpassbarkeit an die Situation und die Zusammenarbeit.
- Genaue Kenntnis der digitalen Abhängigkeiten und wie diese die eigenen Kernprozesse und die der Partner beeinflussen hilft bei der Reaktion auf Sicherheitsvorfälle.
- Ziel des Krisenmanagements bei IT-Sicherheitsvorfällen muss sein, das digitale Ökosystem im weiteren Sinne funktionsfähig zu erhalten. Resilienz von Sytemumgebungen ist von Beginn an mitzuplanen.
- Beim Krisenmanagement benötigt man vielfältige Fähigkeiten und Kompetenzen: Technologie, Kommunikation, Verhaltenspsychologie.
- Konstruktive und nahtlose Zusammenarbeit.
- Kommunikation mit allen Beteiligten und öffentliches Risikomanagement. Transparenz gegenüber allen Stakeholdern wird aktiv eingefordert.

- Flexible und zukunftsorientierte Architekturen mit strategischer Autonomie.
- Sie brauchen klare Verantwortlichkeiten mit eindeutiger Führung. Erfolgreiches Krisenmanagement erfordert einen breit angelegten und überprüften Krisenreaktionsplan, der vom ersten Moment der Krise umgesetzt wird. Ein eindeutiges Mandat, zentrale Verantwortung und die Autorität, das Krisenmanagementprogramm zu entwickeln ist unerlässlich.
- Dabei kann es je nach kulturellem und historischem Hintergrund durchaus unterschiedliche Lösungen geben. Allerdings gleichen sich die Normen und Erwartungen immer mehr an. Darüber muss man sich bewußt sein, da IT-Sicherheitskrisen heute selten lokal oder regional sind und die Abhängigkeiten verschiedene Kulturräume betreffen.