Cyber Security: Technology Innovation vs. Cyber Resilience

Speaker: **Bosco Novak, Rohde & Schwarz**

Date: **Luzern, 17 October 2018**

Event **Eröffnung Studiengang BSc Information & Cyber Security**

Heute hier zu stehen und vor Ihnen vortragen zu dürfen – es ist eine große Ehre für mich und auch eine große Freude.

Information Security und Cyber Security – dies ist eine der größten Herausforderungen für unser Gesellschaft, unabhängig davon, ob wir eine staatliche Verantwortung tragen, in einem Unternehmen agieren oder dieser als Bürger begegnen. Wir stehen erst am Anfang, tatsächlich zu begreifen, wie groß diese Herausforderung sein wird. Demut ist angebracht. „Ich weiss, dass ich nichts weiss“ ist eine zutreffende Aussage.

Investitionen in Technologie, Investitionen in die Infrastruktur, in die Prozesse – all dies ist notwendig. Am Wichtigsten jedoch sind die Investitionen in Kompetenz, in die Menschen, die Spezialisten, welche die Zukunft gestalten und mitbestimmen.

Sie verstehen jetzt, warum ich mich freue, heute bei der Eröffnung Ihres Studienganges hier sprechen zu dürfen.

Digitale Souveränität und Cyber Resilience

„Souveränität“ ist ein bedeutendes Konzept.

Im Völkerrecht bedeutet Souveränität, dass jede Nation innerhalb ihrer Grenzen – als souveräner Staat – die Hoheitsgewalt hat, also entscheiden darf, was innerhalb dieser Grenzen passiert. Deswegen haben wir Gesetze, deswegen haben wir eine Exekutive, wie z.B. die Polizei oder das Militär, die nicht nur sicherstellen, dass die Gesetze eingehalten werden, sondern auch, dass die Grenzen verteidigt werden, dass der Bevölkerung kein Schaden zustößt und dass Eindringlinge gestoppt werden.

Dieser Begriff der Souveränität bezieht sich übrigens nicht nur auf die geographischen Grenzen und materielle Werte. Schon seit jeher spricht man davon, dass „Staatgeheimnisse“ geschützt werden, also immaterielle Güter.

Heutzutage hören wir nun häufig den Begriff der „Digitalen Souveränität“.

Das Konzept der Souveränität lässt sich 1:1 übertragen auf den Schutz der Informationsräume, den Schutz von Daten und Kommunikation seiner Bürger im Cyberraum.

Im Gegensatz zur „klassischen Souveränität“ stehen wir jedoch bei der „Digitalen Souveränität“ noch am Anfang.

- Wie definiere ich einen Informationsraum?
- Was bedeutet es, wenn Daten in der Cloud sind? Wo befindet sich die Cloud?
- Welche Sicherheitsschlüssel werden genutzt, um den Informationsraum, ggf. sogar die Cloud abzusichern?
- Was bedeutet eigentlich „Schäden im Informationsraum vermeiden“ – was bedeutet im Informationsraum „Wiederherstellen eines normalen Zustandes?“

Hier ist vieles in Bewegung – und wird auch in Bewegung bleiben, und daher gibt es logischerweise noch viele Fragezeichen, auf die wir erst im Laufe der Zeit Antworten finden werden.

Den Begriff der „digitalen Souveränität“ kann man unmittelbar auf die Unternehmenswelt sowie den privaten Bereich übertragen. Natürlich müssen wir unsere eigenen Informationsräume schützen, seien es die persönlichen Kontodaten im Haushalt - oder in einer Firma die Daten der Finanztransaktionen – bis hin zu Technologie- und Produktdaten in der Entwicklung.

Es ist interessant, die Lernkurven zu beobachten. Noch vor ein paar Jahren sprachen wir alle von „Network und Intrusion Protection“, von „Fire walls, black lists, white lists“. Wir fokussierten auf den Schutz der Informationsräume. Inzwischen hat sich der Blickwinkel weit geöffnet. Wir haben begriffen, dass es naiv ist, zu denken, man kann 100%-en Schutz darstellen.

Unzählige Cyber Attacken geschehen täglich und zahlreiche Cyber Attacken sind erfolgreich. Wir müssen uns also mit der gleichen Priorität auf die Handhabung eines erfolgreichen Angriffs fokussieren, auf das Wiederherstellen eines Minimum Betriebes, auf das Beseitigen von Schäden, dem Entfernen von Eindringlingen. Wir nennen dies Cyber Resilience. Dieses Konzept steht heute ebenso im Fokus, wenn es um die Konzepte für digitale Souveränität im Cyberraum geht.

Innovation

Der Titel meines Vortrages lautet „Technology Innovation vs. Cyber Resilience“. Lassen Sie mich also jetzt der „Innovation“ zuwenden.

„Innovation“ ist ein tolles Wort; ich verbinde „Innovation“ mit vielen positiven Emotionen, mit Dynamik, mit Leidenschaft – bis hin zur Gänsehaut, wenn man an einer Spitzeninnovation verantwortlich mitwirken darf.

Bei Rohde&Schwarz sind wir bei allen neuen Mobilfunkstandards dabei. Wenn ich richtig gezählt habe, sind in diesem Raum ca. 200 Menschen. Zusammen haben wir ungefähr

300 Smartphones – davon sind mindestens 150 Smartphones mit einem Rohde&Schwarz Messgerät getestet worden, bevor diese in Ihre Hände gelangten.

Für uns ist Innovation Teil unserer DNA. Wir sind mit unseren Geräten in allen Laboren dieser Welt; wir arbeiten mit bei autonomem Fahren, bei multimedialen Streaming Technologien, bei der Drohnenabwehr, bei digitaler Mustererkennung, bei Cyber Technologien, Crypto-Algorithmen und künstlicher Intelligenz. Dabei kommt es uns darauf an, dass aus der Innovation auch immer ein Produkt resultiert. „Make Ideas Real“ sagen wir intern.

Was bedeutet aber eigentlich Innovation?

Innovation ist etwas Neues. Es ist etwas, was wir vorher noch nie gemacht haben - und ich weiß nicht, wie es Ihnen geht, aber bei mir persönlich ist es so, wenn ich etwas Neues mache, etwas, was ich noch nie gemacht habe - dann geht auch vieles schief, von 10 Versuchen scheitere ich bestimmt sechs oder sieben Mal --- aber das ist eben in der Natur von Innovation.

Man kann es auch anders sagen: Wer Innovation ernst nimmt, der ist bereit zu experimentieren und hat Durchhaltewillen und den unbedingten Willen zum Erfolg.

“Cyber Resilience produced by trusted Technology Innovation”

Nun aber zurück zur „Digitalen Souveränität“ und „Cyber Resilience“.

Es ist einfach daher gesagt: *„Wir müssen bei der Cyber Resilience technologisch innovativ sein, ansonsten können wir den Cyber Attacken nicht standhalten.“*

Die meisten werden bei dieser Aussage nicken – aber das legt sich schnell, wenn wir dies anders formulieren: „*Im Bereich Digitale Souveränität und Cyber Resilience experimentieren wir gerade rum“.* Ich bin überzeugt, Sie werden niemanden finden, der dies spontan unterstützt.

Der Weg nach vorne wird jedoch sehr klar, wenn wir - nur für einen Moment - die Rolle des Angreifers einnehmen, desjenigen, der die Cyber Attacke fährt. Der Angreifer nutzt ohne Scham jegliche technologische Innovation. Für ihn geht es nicht darum, 100%ge Cyber Security darzustellen, immer vorhersagbare Ergebnisse zu erzielen. Im Gegenteil, es muss nur ein einziger Angriff erfolgreich sein. Für den Angreifer ist Innovation die Basis.

Für uns gilt: Innovation in der Cyber-Attacke müssen wir mit innovative Lösungen der Cyber Security begegnen.

Wir sehen inzwischen alle Formen von Cyberattacken, bis hin zu ersten Einsätzen von künstlicher Intelligenz. Wenn wir den Umfang und insbesondere die Geschwindigkeit der eingesetzten Datenanalyse und Datenverarbeitung beim Angriff betrachten, wenn wir die

Komplexität der Algorithmen sehen, dann können wir nicht erfolgreich sein, wenn wir versuchen, diese Innovationen mit der „Technologie von gestern“ abzuwehren.

Cyber Resilience kann nur dann erfolgreich sein, wenn wir selbst stets, mit voller Leidenschaft, alle technologischen Innovationen anwenden. Wir müssen bereit sein, zu experimentieren, und wir müssen verstehen, was es bedeutet, wenn wir Experimente machen. Damit dies erfolgreich ist, brauchen wir eine weitere Komponente: Vertrauen.

Bei mir heißt das: “Cyber Resilience produced by trusted Technology Innovation“.

„Trust“ fängt beim Vertrauen zum Technologiepartner an. Wir haben alle vor zehn Tagen den Bloomberg Artikel gelesen, über die Befürchtung, dass ein Chip-Komponenten Lieferant systematisch Backdoors in viele High-Tech Artikel eingebaut hat.

Solchen Gefahren kann man nur entgehen, wenn man bewusst und transparent vertrauenswürdige Technologie Partner auswählt. Dazu gehört natürlich auch, dass die darunterliegende Wertschöpfungskette auditiert und transparent ist.

Wichtige Kriterien sind die Transparenz der Entwicklungs-und Produktionsprozesse, die Möglichkeit, unangekündigt tiefgehende Audits durchzuführen, ein regelmäßiges, transparentes Berichtswesen, Klarheit über die Prozesse, insbesondere über HR Prozesse: „Wie werden Mitarbeiter ausgewählt und Sicherheit überprüft?“ „Gibt es ein umfangreiches Trainingsprogramm“ „Welche Unternehmenskultur liegt vor?“

Technologisch gibt es viele Ansätze. Wir sprechen von „Security by Design“, d.h. wir analysieren natürlich, welche Elemente besonders sicherheitsrelevant sind. Diese müssen separiert werden und speziell abgesichert sein. Sogenannte Security Hardware- und Software Anker sind mittlerweile Standard bei den wesentlichen Firmen.

Wir schauen uns die Architektur an. Wie können wir gewisse Bereiche so segmentieren, dass ein erfolgreicher Cyber Angriff eben nur eine begrenzte Wirkung hat? Wie reduzieren wir Angriffsfläche generell?“

Es hat sich inzwischen ein De-facto Standard entwickelt, der beschreibt, welche Technologieunternehmen dem Anspruch des „Vertrauenswürdigen Technologiepartners“ genügt.

Um jedoch vertrauenswürdige Innovation tatsächlich erfolgreich in der Cyber Resilience einzusetzen, bedarf es einer soliden, nachhaltigen eigenen Kompetenz. Ohne einen Kern an Experten ist es unmöglich, die intensiven und transparenten Dialoge mit Technologiefirmen zu führen, zu beurteilen, wer von uns tatsächlich Innovationen beitragen kann und wer auch nur „mit Wasser kocht“. Die Investitionen in Technologie und eigener Kompetenz Entwicklung müssen Hand in Hand gehen. Dies muss, wie wir heute erleben dürfen, im Zusammenschluss von öffentlicher Hand, Forschung und Lehre sowie der Industrie geschehen.

Summary

Digitale Souveränität erfordert den konsequenten Aufbau der Fähigkeiten zum Schutz der Informationsräume vor Angriffen und zum Wiederherstellen des Status Quo, wenn ein Angriff tatsächlich erfolgreich ist: Die Fähigkeit zu Cyber Protection und Cyber Resilience.

Innovationen müssen integraler Bestandteil der Cyber Strategie sein; dabei ist die intensive und transparente Zusammenarbeit mit vertrauenswürdigen Technologie-partnern die Grundlage einer nachhaltig erfolgreichen Cyber Sicherheit.

Wir feiern heute hier an der Universität Luzern den neuen Studiengang „Information & Cybersecurity“, in dem die nächste Generation von innovativen Experten heranwachsen kann, mit Raum zum Experimentieren. Dies ist der Beginn einer Reise - eine Reise, die wir gemeinsam beschreiten und die wir vor allem gemeinsam gestalten und so den zukünftigen Herausforderungen begegnen. dürfen.