Workshop 5: Cyber Range Trainings in Bezug auf die Widerstandsfähigkeit kritischer Infrastrukturen

Kritische Infrastrukturen sind ein wichtiger Bestandteil unserer Gesellschaft und gleichzeitig populäres Angriffsziel, v.a. wenn es um die darunter liegenden IT-Infrastrukturen geht. Um für diese Angriffe gewappnet zu sein und im Ernstfall auf Bedrohungen adäquat reagieren zu können, stellen Trainings in Cyber Ranges ein geeignetes Instrument dar. Aus diesem Grund war Workshop 5 geprägt von dem Vorhaben, Anbieter von Cyber Range Trainings mit Betreibern kritischer Infrastrukturen zusammen zu bringen, um die Trainingsbedarfe im Bereich KRITIS zu identifizieren und mögliche Umsetzungen in Cyber Ranges zu diskutieren.

Der Workshop bestand aus zwei Teilen – Impulsvorträgen gefolgt von einer Paneldiskussion. Vorbereitet wurde der Workshop von Matthias Schopp, Sebastian Leuck und Ivana Buntic-Ogor vom FI CODE. Die Paneldiskussion wurde von Tim Mittermeier, Head of Red Teaming & Penetration Testing bei Oneconsult, moderiert. Zu Beginn wurden vier Vorträge von Stakeholdern aus dem Bereich Cyber Range Trainings für kritische Infrastruktur gehalten. Zunächst sprach Dr. Jörn Leonhardt vom Bayerischen Landeskriminalamt über die bis dato zu kurz gekommenen Trainingsmöglichkeiten für die Polizei im Bereich Cybercrime und deren Anforderungen an zukünftige Trainings. Hierbei sei es notwendig, aktuelle Kill-Chains und einzelne Techniken zu trainieren, vor allem aber etablierte Prozesse zu üben bzw. Probleme in deren Abläufen zu identifizieren. Darüber hinaus sollte in Trainings nicht ausschließlich die technische Seite beleuchtet werden, sondern diese mit einer Storyline ergänzt werden, um so den Realitätsgrad zu erhöhen und alle beteiligten Rollen mit einzubinden. Zusätzlich betonte Dr. Leonhardt die Wichtigkeit von regelmäßigen Trainings.

Anschließend daran stellte Heinz Marien von der Voith SE & Co. KG die steigenden Anforderungen an Cyber Security im Bereich von Kraftwerkleitsystemen vor. Eines der Themen war die IT-OT-Konvergenz. Laut Herr Marien würde die Komplexität der eingesetzten Tools immens steigen, was die Anforderung nach sich ziehe, dass das Personal, das diese Tools installiert, betreibt und wartet dementsprechend ausgebildet und qualifiziert sein muss. Dies könne u.a. durch Trainingsmaßnahmen in Cyber Ranges erreicht werden. Geübt werden sollen sowohl vorbeugende, erkennende, als auch eindämmende Maßnahmen. Zu den vorbeugenden Maßnahmen zählten beispielsweise Prozesse beim Kunden. Bei den erkennenden Maßnahmen ginge es um das Training im Umgang mit Tools wie Intrusion Detection Systemen. Bei den eindämmenden Maßnahmen handle es sich um Themen, wie dem Üben von Notfallmaßnahmen.

Gefolgt wurde dies von einem Vortrag von Gregor Langner von der Cyber Range des Austrian Institute of Technology. Ein geschätzter Vorteil von Trainings in Cyber Ranges sei, dass man Fehler machen und Dinge ausprobieren dürfe, die man in produktiven Umgebungen nicht machen könne. Laut Herrn Langner zeichne sich ein gutes Szenario dadurch aus, dass es die Realität widerspiegelt. Jedoch müssten nicht 1:1 dieselben Technologien darin enthalten sein, wie sie in der Realität vorkommen. Teilnehmen an Cyber Range Trainings sollten sowohl technisches als auch nicht technisches Personal. Auch in diesem Vortrag wurde betont, dass Prozesse, Teil derer auch Kommunikationswege sind, trainiert werden sollen.

Zum Abschluss der Vortragsreihe sprach Dr. Cora Lisa Perner von Airbus Defence and Space darüber, wie Virtualisierungs- und Simulationslösungen genutzt werden können, um das notwendige Wissen für die Entwicklung, Wartung und den Betrieb von komplexen und sicherheitskritischen Systemen zu erlangen. In diesem Zusammenhang stellte Dr. Perner die

Baukastenlösung von Airbus für Cyber Ranges vor, mit welcher Szenarien per Drag and Drop erstellt werden können.
Im zweiten Teil des Workshops folgte eine moderierte Diskussion zwischen den ReferentInnen. Die Hauptfragestellung der Diskussion war, wie bestehende Cyber-Range-Ansätze verbessert werden können, um die Trainingsbedarfe im Bereich KRITIS zu decken.

Zunächst wurde die Frage aufgeworfen, wo Cyber Range Training im KRITIS Bereich überhaupt notwendig sei. Dies sei vor allem für die „aktive Phase", also für den Fall, dass man einen Sicherheitsvorfall hat, wichtig, da dies aktuell zu kurz komme. Hierbei müssten Notfallmaßnahmen trainiert werden. Außerdem müssten Trainings regelmäßig wiederholt werden. Es gehe somit also nicht rein um technische, sondern auch organisatorische Maßnahmen und Prozesse.

Anschließend daran wurde gefragt, was ein CR-Produkt oder Training für den KRITIS / Operational Technology Bereich leisten müsse und ob dies aktuelle CR-Produkte bereits könnten. Von der Industrie wurde der Wunsch geäußert, dass Trainings anwendungsfreundlich gestaltet werden und ähnlich wie ein E-Learning einfach aufrufbar sein sollten. Außerdem sollten diese so handhabbar sein, als würde man mit seinen direkten Systemen trainieren, ohne großes Abstraktionsvermögen besitzen zu müssen, um das Trainierte in die Realität umsetzen zu können. Die Antwort der CR- Anbietenden lautete, dass direkt in technische Trainings einzusteigen aus ihrer Sicht nicht sinnvoll sei. Stattdessen solle man im Vorlauf via Pen & Paper oder Table-Top-Übungen die tatsächlichen Bedarfe ermitteln. Dabei müsste analysiert werden, bei welchen Prozessen es sinnvoll ist, diese in CR-Trainings abzubilden und auf technischer Ebene müsste bewertet werden bis zu welchem Detailgrad die Abbildung der realen Netze zu erfolgen hat. Dies sei vor allem anwendungs- und zielgruppenspezifisch.

Aus dem Auditorium wurde gefragt, in welcher Umgebung diese Trainings stattfinden, also ob es sich hierbei beispielsweise um Trainingszentren handelt. Außerdem wurde nach dem möglichen Einfluss gefragt, den man als Kunde auf die Planung von Szenarien habe. Aus den Reihen der CR-Betreibenden wurde geantwortet, dass die Trainings nicht zwingend in dedizierten Schulungsräumen stattfinden müssten, sondern teils auch Remotezugriff auf die Übungsumgebung möglich sei. Auch das Beeinflussen der Szenarien seitens der Trainingsinteressenten sei möglich. Allerdings gehe es bei der Trainingsgestaltung nicht nur um Angriffsvektoren, sondern auch um didaktische Aspekte und darum, die Grenzen des Möglichen in Trainings zu kennen.

Die Teilnehmenden der Runde diskutierten außerdem darüber, welches Bedrohungsszenario problematischer und relevanter für Trainings sei – Sabotage oder der Zugriff auf IT- oder OT-Systeme. Im Rahmen von CR-Trainings solle der Fall trainiert werden, wenn jemand in die Anlage eindringt und von innen heraus versucht die Systeme zu manipulieren. Alles, was von außen kommt, wie beispielsweise ein durchgeschnittenes Kabel, sollten Bedrohungen sein, die beim Design der Systemarchitektur bereits berücksichtigt wurden oder ggf. als tolerierbare Risiken eingeordnet wurden. Es solle vor allem das Erkennen von Vorfällen trainiert werden, um weitere Schritte einleiten zu können.

Aus dem Publikum wurde des Weiteren Interesse bekundet, inwiefern man den Ausbildungsstand nach so einem Training nachweisen bzw. zertifizieren könne. Das AIT mache zunächst nach jedem Training eine Feedbackrunde, in der die Einschätzung der Teilnehmer

abgefragt werde, was sie denken, dass während des Angriffs passiert wäre und ihnen aufgezeigt wird, wie der Angriff eigentlich abgelaufen ist. Danach werde ein Report mit Handlungsempfehlungen erstellt und an die Teilnehmenden herausgeben. Wenn es um einen Nachweis für bzw. das Messbarmachen von Resilienz geht, müsse zuerst eine Baseline definiert werden, mit der der Fortschritt verglichen werden könne. Außerdem müsse wahrscheinlich die Gesamtperformance des Teams und nicht der individuellen Teilnehmer bewertet werden. Als Anmerkung wurde aus dem Publikum eine aktuelle Forschungsarbeit der Cyber Range ICE&T des FI CODE erläutert. Diese hätte zum Ziel den Erfolg eines Trainings messbar zu machen. Unter dem Oberbegriff Resilienz sei ein Prozess entwickelt worden, der im Vorfeld eines Trainings zusammen mit der zu trainierenden Partei ermittle, welche Prozesse das Trainings abbilden soll. Daraus würden Kennzahlen (KPIs) abgeleitet, welche eine Bewertung ermöglichen sollen. Die abgeleiteten KPIs würden im Training erfasst werden, wodurch zum einen die Möglichkeit entstehe, eine Baseline zu ermitteln und zum anderen, bei wiederkehrenden Trainingsparteien die Fortschritte hinsichtlich der Resilienz gemessen würden.

An Dr. Leonhardt wurde die Frage gerichtet, zu welchen Fällen die Cyberpolizei überhaupt gerufen wird und welche Wünsche die Polizei an Cyber Range Trainings hat. Bei den Fällen, zu denen die Polizei gerufen werde, handle es sich hauptsächlich um Ransomware-Vorfälle, da andere Incidents (z.B. Malicious Insider) meist intern geklärt würden. Für die Polizei sei ferner die dynamische Lage während eines Trainings weniger interessant – es ginge vorwiegend um statische Trainings. In der Realität würde es meist so aussehen, dass beim Eintreffen der Polizei bereits die angegriffenen Systeme vom Netz getrennt seien. Im besten Fall würden sie in Trainings fertige Netzinfrastrukturen bekommen, in denen verschiedenste Szenarien gespielt werden können, da sie auch in der Realität unterschiedliche Netztopologien vorfinden würden. Es wurde nochmals die Wichtigkeit der verschiedenen Rollen der Cyberpolizei, wie Ermittler oder Forensiker, betont und dass für erstere v.a. die gesamte Storyline neben den technischen Aspekten im Vordergrund stehe. Deshalb sei der Aufbau von Trainings als Planspiel sinnvoll, bei der auch die Kommunikation geübt werde. In der Realität sei die Strafverfolgung für das angegriffene Unternehmen meist zweitrangig. Dadurch werde die Polizei eher als Störfaktor wahrgenommen – sie versuche aber ihre Arbeit so zu machen, dass so wenig wie möglich in den Wiederherstellungsprozess eingegriffen werde. Bei den meisten Fällen gebe es keine perfekte Spurenlage. Stattdessen werde die Polizei meist zu spät gerufen, wodurch viele Spuren nicht mehr vorhanden oder kaum noch zuzuordnen seien.

Dies warf die Frage bezüglich der Relevanz von Aktualität in Cyber Range Trainings auf. Die Diskussionsteilnehmenden waren sich bezüglich der Aktualität von Trainingsinhalten uneinig, also ob es besser wäre, auf Systemen zu üben, die für aktuelle Exploits angreifbar sind oder auf teils veralteten Systemen, wie sie jedoch oft im Bereich der kritischen Infrastruktur eingesetzt werden. Wenn es beispielsweise eher um das Trainieren von Methoden geht, die sich mittelfristig gesehen nicht stark ändern, sei die Verwendung von älteren Systemen akzeptabel. Wenn es allerdings um die genutzten Kill-Chains geht, kam der Wunsch auf, dass diese möglichst aktuell gehalten werden. Als Tenor kann mitgenommen werden, dass die zu verwendenden Systeme und Schwachstellen innerhalb von Cyber-Sicherheitsübungen vom jeweiligen Trainingsziel abhängig gemacht werden sollten.

Eine weitere Frage, die aufkam war, wie man verwendete Systeme (Switches, Firewalls, Router, etc.) virtualisieren könne und wie die Lizenzierung dabei funktioniere, wenn man die IT-

Umgebung eines Trainingskunden nachbaut. Je nach Cyber Range Produkt ist diese Frage unterschiedlich zu beantworten. Die AIT Cyber Range verwende beispielsweise lediglich lizenzfreie Produkte, mit der Ausnahme, dass auch lizenzpflichtige Produkte integriert werden können, wenn der Kunde sie für das Training zur Verfügung stellt. Hierbei ist aber ebenso zu beachten, was die Zielsetzung des Trainings ist, ob es um ein bestimmtes Verhalten geht, das ich trainieren möchte (wie reagiere ich auf einen „Alert"), oder ob es um den Umgang mit einem konkreten Produkt geht. Außerdem ist es, je nach CR-Produkt auch möglich, bei Hardware, diese direkt an die CR-Umgebung anzubinden, ohne diese zu virtualisieren.

Ein zusätzlicher Aspekt war die fortschreitende Vernetzung und die Fragestellung, ob über die Cloudtechnologie neue Angriffsvektoren möglich wären. Eine Möglichkeit, die Risiken zu minimieren, sei es, Cloudlösungen nicht für betriebsrelevante Anwendungen direkt zu nutzen, sondern nur Funktionen auszulagern, die zur Optimierung des Betriebs oder zur Wartung der Anlage beitrage. Trotzdem müssten Maßnahmen getroffen und Kontrollmechanismen eingebaut werden, um die Ausnutzung als initialen Angriffsvektor zu verhindern und zu detektieren. Cloudservices sollten demnach lediglich über eine DMZ angebunden werden. IT, die in der Cloud steht, müsse als externe Schnittstelle behandelt werden.

Da IT und OT nicht mehr voneinander trennbar sind stellt sich auch für Cyber-Range-Anbieter die Frage, wie damit im Rahmen von Trainings umgegangen werden kann. Laut der Anbieter sei eine Cyber Range lediglich ein Werkzeug, eine Abstraktion der Realität und man müsse die Frage danach, was man abbildet, abhängig vom Übungsziel machen und auf die nötigsten Komponenten reduzieren. (In der CR wird alles was von außen kommt oft als Interface dargestellt, über das Daten reinkommen -> es geht im CR-Kontext vorrangig um die Daten und weniger darum, ob das eine Antenne ist, ein Beacon, oder Cloud, etc...)

(Frage aus dem Publikum) Da davon auszugehen ist, dass in Zukunft immer mehr IT für OT genutzt werden wird und sich daraus neue Schwachstellen ergeben werden, ist es möglich, dass man dies in die Cyber Ranges mit einbaut und gegebenenfalls auch schon vorausschauend Best Practices daraus entwickelt?
Einschätzung: Es ist immer möglich Annahmen zu treffen und Vermutungen zu implementieren, jedoch daraus Best Practices oder Standards zu entwickeln ist schwierig, da man nichtsdestotrotz nicht weiß, wie die Zukunft aussehen wird.

Außerdem stellt sich die Frage, ob sich die Vorbereitung von CR-Szenarien für KRITIS überhaupt stark von nicht-KRITIS Szenarien unterscheidet.
Durch die Range-Betreiber wurde erläutert, es sei wichtig, jemanden mit Domänenwissen zu haben, der wisse wie die benötigten Systeme funktionieren. Unabhängig vom cyber-physikalischen System sei die Ansteuerung jedoch meist gleich. Somit müsste lediglich die Front-End-Darstellung dahingehend gestaltet werden, dass dieses in den Augen der Teilnehmer realistisch erscheint.
Aus dem Publikum wurde darauf Bezugnehmend gefragt, ob es hierbei Unterschiede zwischen der IT und OT Welt gäbe, da bereits die Aussage getätigt wurde, dass die Verwendung genau der gleichen Systeme aus dem bekannten IT Netz der Trainingsteilnehmer nicht von primärer Bedeutung sei für den Lerneffekt.
Aus Sicht des AIT wurde hier grundsätzlich die gleiche Aussage getätigt, jedoch mit der Einschränkung, dass es Spezialfälle gäbe, in denen die Systeme entsprechend abgebildete

werden müssten. Airbus ergänzte, dass es um die Konsequenzen des Verhaltens ginge. Wenn dieses für das Training und Szenario relevant sei, müsse das System abgebildete werden.
Aus dem Publikum wurde ergänzt, dass es für die IT Welt nachvollziehbar sei, ähnliche Systeme zu verwenden, da hier mittlerweile vieles standardisiert sei, wie, z.B. Kommunikationsprotokolle. Es kam jedoch die Frage auf, ob dies auch für die OT Welt gälte, da historisch viele unterschiedliche Protokolle entstanden seien in der Vergangenheit.
Aus Sicht des AIT sei auch hier mittlerweile vieles standardisiert, Herr Marien von der Voith SE & Co. KG ergänzte jedoch, dass es noch einige domänenspezifische und proprietäre Protokolle in der Realität gäbe.

Abschließend wurde noch die Frage gestellt, ob sich je nach Auswirkung eines Angriffs (ein überlaufender Staudamm vs. falsch zusammengesetzte Bauteile) die Herangehensweisen der Polizei unterscheiden würde und deswegen auch Cyber Range Trainings dementsprechend anders gestaltet werden müssten. Als Antwort ließ sich hier festhalten, dass Cyber Ranges letztlich als technisches Framework dienten. Die Entwicklung von Methodiken und Vorgehensweise durch das Training seien für die Arbeit der Polizei wesentlich relevanter als die rein physischen Auswirkungen eines Angriffs.

Zusammenfassend kann gesagt werden, dass den jeweiligen Stakeholdern im Bereich von Cybersicherheitstrainings für kritische Infrastrukturen bewusst sein muss, was ein Training in einer Cyber Range leisten kann und was nicht. Man kann nicht alles in solchen Trainings abbilden und „Kunden“ dieser Trainings sollten sich genaue Gedanken darüber machen, was ihre Trainingsziele sind und von den Betreibern bei der Identifikation dieser unterstützt werden.