Cyber Range: Netzverteidigung trainieren mittels Simulation

Ralf Kaschow[1] · Oliver Hanka[1] · Marcus Knüpfer[2] · Volker Eiseler[2]

[1]ESG Elektroniksystem- und Logistik-GmbH
{Ralf.Kaschow | Oliver.Hanka}@esg.de

[2]Universität der Bundeswehr München
{Marcus.Knuepfer | Volker.Eiseler}@unibw.de

Zusammenfassung

Cyberattacken sind in aller Munde. Eine effiziente Erkennung und Bewältigung dieser Attacken ist jedoch eine Herausforderung. Durch die steigende Anzahl an Geräten, die auch Angriffsziele darstellen sowie die Vielfalt der vorhandenen Tools, die Angreifer nutzen können, wird die Verteidigung des eigenen Netzes zu einer immer größeren Problemstellung und Herausforderung für Netzadministratoren. Hinzu kommt, dass es einen eklatanten Bedarf an gut ausgebildetem Personal im Cyber-Umfeld gibt. Cyber Ranges bieten die Möglichkeit das Fachpersonal zu trainieren und Handlungsabläufe bei einer Cyber-Attacke zu üben. In diesem Paper wird der Einsatz von Cyber Range Lösungen als Mittel zum Training von Personal im Cyber-Umfeld evaluiert. Es werden Anforderungen definiert, welche eine Cyber Range für ein effektives und effizientes Training erfüllen muss. Inwiefern vorhandene Lösungen diese Anforderungen erfüllen, wurde mittels der Durchführung von mehr als 80 Testübungen im operativen Training und der universitären Lehre evaluiert. Die Ergebnisse dieser Evaluierung werden im Folgenden präsentiert.

1 Einleitung

Der Schutz und die Verteidigung von IT- und Kommunikationsnetzen vor Cyberattacken hängen stark von dem kontinuierlichen Einsatz, der Bedienung und dem Monitoring einer Vielzahl von Cybersicherheitsprogrammen und -produkten ab. Die Zielsetzung ist hier die rechtzeitige oder zumindest frühe Erkennung von Anomalien im Netz, welche auf einen Cyberangriff hindeuten und welche Hinweise auf mögliche Schwachstellen geben. Die Reduktion, idealerweise die Elimination, dieser Schwachstellen und somit der Handlungsoptionen von Angreifern muss in der heutigen Zeit die Priorität der Verteidiger sein [CISC17].

Router, Switches, Firewalls, Intrusion-Detection-Systeme, Monitoring-Dienste und verschiedene andere IT-Sicherheitskomponenten sind nur einige der Systeme, die in einem modernen Rechnernetz laufen und von Administratoren und Operatoren verwaltet und überwacht werden müssen. Die Operatoren dieser Systeme können nur in den seltensten Fällen Experten in der Handhabung all dieser Systeme sein. Zusätzlich sind sie durch hochdynamische und sich schnell entwickelnde IT-Infrastrukturen und IT-Dienste herausgefordert.

Ein zweites wesentliches Kriterium für eine wirksame Netzverteidigung ist die Fähigkeit, die Aktivitäten eines Angreifers zu identifizieren, zu isolieren und wieder rückgängig zu machen.

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 126-137.

Dabei kommt es auf ein methodisches und zielgerichtetes Vorgehen an. Es muss sichergestellt werden, dass die „Kontamination“ des eigenen Netzes vollständig beseitig ist.

Dabei geht es nicht alleine darum, Schadsoftware zu eliminieren, sondern beispielsweise auch Datenmanipulationen aufzudecken und zu korrigieren. Bei allen Maßnahmen ist grundsätzlich zu beachten, dass keine Spuren verwischt werden. Nur so wird eine umfassende Bestandsaufnahme ermöglicht, welche die Identität des Angreifers sowie dessen Weg beim Eindringen in das Netz aufdecken soll. Weiterhin ist darauf zu achten, dass die eigenen Gegenmaßnahmen nicht dazu führen, den noch verfügbaren Geschäftsbetrieb unnötig und über die Maßen zu beeinträchtigen oder gar zu unterbrechen.

Das Fehlen von entsprechend gut ausgebildetem Personal verstärkt das Problem, die immer komplexeren IT-Systeme und Netze in geeigneter Weise zu administrieren, zu überwachen und sicher zu betreiben, vor allem vor dem Hintergrund der sich ständig vergrößernden Anzahl an Angriffen auf IT-Infrastrukturen.

Daher ist die Fähigkeit, Werkzeuge und Geräte in einer simulierten / emulierten Umgebung zu testen, Netzarchitekturen zu entwerfen und zu konfigurieren sowie insbesondere das operative Personal auf realistische Weise hinsichtlich unterschiedlicher Bedrohungsszenarien auszubilden und zu trainieren, ein wesentlicher Faktor für die Verbesserung einer Cyberverteidigungsstrategie.

Die Simulation und Operationalisierung von Netzen in sogenannten Cyber Ranges stellt eine effiziente Methode zum Aufbau derartiger Fähigkeiten dar. Eine Cyber Range ist eine virtuelle Umgebung, die für die Entwicklung von IT-Technologien und speziell für das Training mit diesen verwendet wird. Sie bietet Werkzeuge, die zur Verbesserung der Stabilität, Sicherheit und Leistung von IT-Infrastrukturen und Systemen beitragen [FeTO14, PTCB16].

Insbesondere weisen Cyber Ranges das Potenzial zum effizienten Trainieren folgender Prozesse und Kernkompetenzen auf:

- Gewinnen von Handlungssicherheit im Umgang mit IT-Sicherheitswerkzeugen und -produkten
- Erkennen von Anomalien im Netzverkehr und Generieren eines Cyber-Lagebildes (Situational Awareness)
- Identifikation von Angriffen (Attribution) und Angreifern
- Einleitung von Maßnahmen (taktische und operative Reaktion/Prävention)
- Effizientes Teamwork (Herbeiführung und Aufrechterhaltung der Initial und Full Operation Capability (IOC/FOC))

Die möglichen Zielgruppen von Cyber Ranges sind dabei vielschichtig und nicht auf die IT-Administratoren beschränkt. Computer Emergency Response Teams (CERTs) und Security Operation Center (SOC) Teams können insbesondere die Abläufe und die Zusammenarbeit trainieren. IT-Sicherheitsbeauftragte können praktisch Erfahrungen sammeln, die sie in ihre tägliche Arbeit einbringen können. Ferner stellen Cyber Ranges eine hervorragende Möglichkeit dar, das Personal des in der Bundeswehr neu geschaffenen Kommandos Cyber- und Informationsraum (CIR) und der Abteilung Cyber- und Informationstechnik (CIT) auszubilden und zu trainieren.

Im Rahmen der im Folgenden beschriebenen Evaluierung wurde untersucht, welche Anforderungen die Trainingsanwendung an eine Cyber Range stellt und inwieweit vorhandene Cyber-

Range-Lösungen diese Anforderungen erfüllen können. Hierzu wird in Kapitel 2 zunächst die Related Work im Themenbereich zusammengefasst. Im Anschluss werden in Kapitel 3 Ablauf und Ziele der Evaluierung beschrieben, deren Ergebnisse in Kapitel 4 zusammengefasst sind. Aus der Evaluierung abgeleitete Kernaussagen und Use Cases werden in Kapitel 5 dargestellt. Kapitel 6 gibt zum Abschluss einen Ausblick auf zukünftige Aktivitäten.

2 Related Work

Der Begriff der Cyber Range hat sich aus dem militärischen Jargon entwickelt. Der IT-Spezialist soll auf einer solchen Cyber Range vergleichbar trainieren können wie ein Soldat auf einer Shooting Range (Schießbahn). Gleichzeitig soll diese Umgebung aber auch das Experimentieren an und Testen von IT-Sicherheitsprodukten unterstützen [DaMa13].

Auf dieser Grundlage existieren eine Reihe von Projekten, welche sich mit diesem Thema auseinandersetzen. Ein Beispiel ist die National Cyber Range [FeTO14]. Initiator dieser Cyber Range ist die Defense Advanced Research Projects Agency (DARPA), welche im Auftrag des US-Verteidigungsministeriums Forschungsprojekte für die Streitkräfte durchführt. Der Fokus dieses Projekts liegt in der Schaffung einer Umgebung, in der IT-Systeme und Vorgehensweise getestet werden können. Davis et al. fassen in ihrer Arbeit [DaMa13] 30 öffentlich bekannte Cyber Ranges und Cyber-Testumgebungen zusammen, welche alle einen vergleichbaren Fokus haben. Dabei haben viele Cyber Ranges einen sehr eng gefassten Einsatzzweck, welcher vor allem das spezielle Testen von einer Art von Systemen ermöglicht [Wint12]. Das Trainieren und die Ausbildung von Einzelpersonen und Teams in der Netzverteidigung ist bei den zusammengefassten Arbeiten in diesem Abschnitt nur ein Randthema. Im Gegensatz dazu steht in der vorliegenden Arbeit dieses Training im Mittelpunkt der in den nachfolgenden Abschnitten aufgeführten Evaluierung von Cyber-Range-Lösungen.

Das Training von Personen im Bereich der Cyber- und IT-Sicherheit wird bei der Durchführung von großen Übungen in den Vordergrund gestellt. Die vom NATO Cooperative Cyber Defence Centre of Excellence entwickelte Cyber Range in Estland bildet die Grundlage für die seit 2010 jährlich durchgeführte NATO Übung *Locked Shield* [NATO16]. Trainingsteilnehmer dieser Übungen stammen aus den verschiedenen Nationen der NATO sowie deren Partnerstaaten. Einen vergleichbaren Ansatz wählt die European Union Agency for Network and Information Security (ENISA), welche mit der Übung *Cyber Europe* [ENIS16] seit 2010 im Abstand von zwei Jahren regelmäßig eine langfristig angelegte paneuropäische Übung durchführt. Im Jahr 2016 beteiligten sich zuletzt 26 Nationen. Diese Übungen haben gemein, dass sie die Zusammenarbeit unterschiedlicher Personen bei Cyberangriffen trainieren und verbessern soll. Hierfür wird neben der Cyber Range eine Kommunikationsinfrastruktur zur Verfügung gestellt, welche für die Teilnehmenden untereinander gedacht ist sowie die Kommunikation der Organisierenden mit den Teilnehmenden ermöglicht. Mit der Bereitstellung und den technischen Herausforderungen solcher Übungen beschäftigen sich unter anderem die Cyber Range Interoperability Standards Working Group des US-Verteidigungsministeriums [DaCo15, DaSm15] sowie Celeda et al. [CCVT15]. Aufgrund der Größe der Übungen und der Anzahl der beteiligten Nationen liegt bei diesen Einsätzen einer Cyber Range der Fokus klar auf dem taktischen Arbeiten und der Kooperation der multinationalen Partner und weniger auf den operativen Tätigkeiten des IT-Fachpersonals und dessen Zusammenarbeit als Team, was wiederum Schwerpunkt der in der vorliegenden Arbeit aufgeführten Evaluierung ist.

Bereits Yurcik et al. [YuDo01] haben festgestellt, dass die Ausbildung von IT-Sicherheitspersonal ein großes Problem darstellt. Bei ihrem Vergleich unterschiedlicher Ausbildungsansätze heben sie das aktive Lernen mittels der praktischen Durchführung von Angriff und Verteidigung in isolierten Laborumgebungen als die „Zukunft der Information Security Ausbildung“ [YuDo01] heraus. Eine Umsetzung dieser Lehrmethode stellen sogenannte Capture-The-Flag-Veranstaltungen dar. Hierbei werden den Teilnehmenden Aufgaben gestellt, welche unter anderem mittels IT-Angriffstechniken gelöst werden können. Auf diese Weise lernen Teilnehmende die zu verteidigenden IT-Systeme spielerisch aus Sicht eines Angreifers kennen und können Rückschlüsse auf notwendige Verteidigungsmöglichkeiten ziehen. Ein Überblick über diese Lehrmethode ist unter anderem in [BoSB15] zu finden. In der hier beschriebenen Evaluierung ist diese Herangehensweise nur am Rande erwähnt, da der Fokus auf dem Trainieren der Netzverteidigung liegt.

SIMOC [MaCR15] stellt einen Cyber-Simulator dar, welcher für das brasilianische Militär entwickelt wurde und das praktische Training der Netzverteidigung ermöglicht. Machado et al. beschreiben in ihrer Veröffentlichung den Aufbau einer Cyber Range und gehen auf notwendige Aspekte aus Sicht der Technik und des Trainings ein. Die beschriebene Evaluierung bezieht sich auf die Eindrücke der Trainer und den notwendigen Umfang für die Erstellung von Übungsaufgaben unterschiedlicher Größe und Komplexität. Unser Ansatz der Evaluierung ist dahingehend umfassender, da die Zielgruppe des Trainings im Mittelpunkt steht sowie die Zusammensetzung dieser Gruppe nicht nur auf das Militär beschränkt, sondern weiter gefasst ist.

Auf eine breite Zielgruppe ausgelegt ist ebenso die Cyber Range CyRIS des Japan Advanced Institute of Science and Technology [PTCB16]. Die Autoren gehen dabei in ihrer Veröffentlichung auf das einfache Erstellen und Vervielfältigen gekapselter Cyber-Range-Umgebungen ein. Auf diese Weise wird es effizient ermöglicht einer größeren Anzahl von Teilnehmern eines Trainings eine eigene Umgebung zur Verfügung zu stellen. Zum aktuellen Zeitpunkt beschränken sich die Implementierungen auf zwei virtuelle Maschinen pro Umgebung, welche bis zu 60 Mal vervielfältigt wird. Dieser Ansatz eignet sich gut, um einer Vielzahl an Teilnehmenden IT-Sicherheitsfähigkeiten gleichzeitig zu vermitteln. Ein Ziel unseres Ansatzes ist jedoch, neben den Einzelfähigkeiten auch das Teamwork einer Gruppe zu trainieren.

Seit wenigen Jahren existieren kommerzielle Cyber-Range-Lösungen auf dem Markt. Bei der Sichtung des Marktes zeigt sich, dass die Cyber-Range-Produkte der Firmen CyberBit Commercial Solutions Ltd [CYBE17] sowie Avnet Data Security Ltd. und Israel Aerospace Industries Ltd. [Fish15] verbreitet Anwendung finden. Diese basieren auf Emulations- / Simulationstechnologien und -methoden und wurden in der nachfolgend beschriebenen Evaluierung mit einbezogen.

3 Ablauf und Ziele der Evaluierung

Im Rahmen dieser Veröffentlichung wird die seit 2016 stattfindende Evaluierung beschrieben. Dabei wurden verschiedene Cyber-Range-Technologien, -Produkte und -Konzepte, welche derzeit weltweit existieren und für die Nutzung zugänglich sind, betrachtet.

Zielsetzung der Evaluierung war,

- die Use Cases einer Cyber Range insbesondere für die Aus- und Weiterbildung von Fachpersonal und im Rahmen der universitären Lehre zu identifizieren und zu untersuchen,

- eine Analyse technischer, organisatorischer und sonstiger Anforderungen an eine Cyber Range in Abhängigkeit der Use Cases durchzuführen,
- unterschiedliche kommerzielle Cyber-Range-Produkte hinsichtlich Erfüllung der Use-Case-Anforderungen zu prüfen,
- unterschiedliche Use Cases in der Praxis zu testen und neue Einsatzmöglichkeiten zu erforschen.

Die Evaluierung sollte damit die Grundlagen liefern, um ein Gesamtkonzept zum Aufbau einer Cyber Range auf Basis erster praktischer Erfahrungen erstellen zu können.

Im Zuge der Evaluierung wurden zwei Cyber-Range-Produkte mit erkennbar hohem Reifegrad herangezogen und in den Testübungen eingesetzt.

Im Rahmen der Evaluierung wurden insgesamt mehr als 80 Testübungen mit zahlreichen unterschiedlichen Institutionen, die potenzielle Nutzer einer Cyber Range darstellen, durchgeführt. Die Institutionen entsandten dazu Übungsteams mit einer Größe von vier bis acht Personen. Mindestanforderungen an die Übungsteilnehmer waren gute Kenntnisse in der Netzwerkadministration und IT-Sicherheitsgrundkenntnisse. Für die Testszenarien wurde in der Simulation des Testaufbaus ein generisches IT-Netzwerk nachgebildet, das alle wesentlichen Komponenten und Bereiche eines typischen Netzwerks in größeren Organisationen repräsentierte. Dabei wurden auf dem Markt gängige IT-Security-Werkzeuge für die Netzwerküberwachung (Firewall, SIEM, …) eingebunden. Drei Angriffsszenarios mit unterschiedlicher Komplexität und verschiedenen Schwierigkeitsgraden standen für Testübungen zur Auswahl: Web Defacement (einfach), SQL Injection (mittel), WMI[1]-Wurm (schwer). Die Szenarien wurden je nach Wissen und Erfahrung der Übungsteilnehmer (ohne deren Kenntnis) ausgewählt.

Eine Testübung bestand aus vier Phasen:

- Einweisung in die Simulationsumgebung und vertraut machen der Übungsteilnehmer mit dem Netzwerk und den IT-Security-Werkzeugen.
- Durchführung der Testübung mit der Aufgabenstellung, den jeweiligen Angriff zu erkennen und zu bewältigen. Die Dauer einer Testübung lag zwischen ein bis sechs Stunden je nach Schwierigkeitsgrad und Skill Level
- Übungsauswertung: ausführliche Besprechung des Verhaltens und der Aktionen der Übungsteilnehmer
- Befragung der Übungsteilnehmer in Bezug auf die Evaluierungsaspekte in Form von Feedbackrunden und Fragebögen

Zur Erlangung eines fundierten Ergebnisses und breiten Meinungsbildes wurde bei der Wahl der Teilnehmer auf eine hohe Diversität geachtet. So wurden die Übungen zunächst unter Beteiligung von Mitarbeitern und Studenten der evaluierenden Organisationen durchgeführt. Im weiteren Verlauf wurde eine Vielzahl unterschiedlicher potenzieller Nutzer aus dem militärischen Umfeld und der privaten Wirtschaft zu Testübungen eingeladen.

Um den Einfluss möglicher nutzer- und branchenspezifischer Rahmenbedingungen und Anforderungen zu untersuchen, wurden potenzielle Nutzer aus den Bereichen öffentliche Verwaltung, Sicherheitsbehörden, Finanzwesen, Verkehrsbetriebe, Energieversorger und Industrieanlagenbetreiber an den Tests beteiligt.

[1] Windows Management Instrumentation

Folgende Kernanforderungen und -fragestellungen in Bezug auf Cyber Ranges wurden in der Evaluierung erarbeitet und anhand der eingesetzten Cyber-Range-Lösungen eingehender untersucht:

- Flexible Modellierung von Netztopologien
- Replikation real existierender Netze – Anforderungen, Möglichkeiten und Grenzen
- Bedarf und Möglichkeiten der Integration von realer HW und SW in die Simulationsumgebung
- Bedarf der Entwicklung von Schnittstellen
- Anforderungen zur Abbildung spezifischer Netze, z. B. militärische Netze, SCADA[2], Automotive
- Simulation von Netzverkehr als realistische Rahmenbedingung für die Anomalie-Detektion
- Flexible Modellierung von Angriffsvektoren und Abbildung von Angriffsszenarien
- Automation von Angriffsszenarien durch einen Attackengenerator
- Performance-Aspekte, z. B. Zeitdauer für den Start und das Zurücksetzen von Übungsszenarien, Systemstabilität
- Unterstützung der Übungsauswertung durch Recording- und Scoring-Systeme
- Übungssteuerungsfunktionen, wie z. B. Rollenmanagement, Übungsdatenmanagement, dynamische Simulationsablaufsteuerung
- Unterstützung durch Graphical User Interfaces
- Traineranforderungen hinsichtlich Fachwissen, Systemexpertise, Methodik und Didaktik
- Betriebsaufwand und Wirtschaftlichkeit
- Datenschutz- und Datensicherheitsanforderungen

4 Ergebnisse der Evaluierung

4.1 Evaluierung aus Sicht des operativen Trainings

An den Testübungen nahmen, neben Einrichtungen der Bundeswehr und Sicherheitsbehörden, Unternehmen aus dem Bereich kritischer Infrastrukturen teil. Diese verteilten sich auf folgende Sektoren: Bankwesen, Industrieanlagen, Transportwesen, Wasser- und Energieversorger, Rechenzentrumsbetreiber sowie Telekommunikation.

Die Übungsteams bestanden, je nach teilnehmender Institution, zum einen aus erfahrenem CERT- und SOC-Personal, sehr häufig aber aus einer Zusammenstellung von unterschiedlichen IT-Administratoren und IT-Security-Personal mit wenig bis fortgeschrittener Erfahrung in der Netzverteidigung.

Folgende Fragestellungen wurden mit den Teilnehmern nach Übungsdurchführung besprochen:

- Welchen Mehrwert sehen Sie in simulationsgestütztem Training, wie es eine Cyber Range bieten kann?
- Welche Use Cases einer Cyber Range sind für Sie von besonderem Interesse?

[2] Supervisory Control and Data Acquisition

- Welche inhaltlichen und funktionalen Anforderungen stellen Sie als Nutzer an eine Cyber Range?

Zusammengefasst wurden die folgenden wesentlichen Aussagen aufgenommen:

Die Möglichkeit, die unterschiedlichsten Angriffsszenarien in realistischer und nachvollziehbarer Form darzustellen, fand bei allen Teilnehmern eine sehr hohe Akzeptanz. Viele Teilnehmer wurden mit für sie neuen Sachverhalten und Herausforderungen im Rahmen von Cyber-Angriffen konfrontiert, welche sie so im Alltag bislang noch nicht erlebt hatten. Dementsprechend wurde der Lerneffekt sehr hoch eingestuft.

Erwartungshaltung aller Übungsteilnehmer ist, dass eine Cyber Range das komplette Spektrum der gängigen Cyber-Angriffe abbilden kann und dieses Abbildungsspektrum einem kontinuierlichen Aktualisierungsprozess unterliegt.

Als primärer Use Case, bei dem die Stärken einer Cyber Range voll zum Tragen kommen, wurde die Durchführung von Cyber-Defence-Übungen angesehen: Bei vielen der teilnehmenden Institutionen waren deutliche Defizite bzgl. Fähigkeiten im Kontext Netzwerkverteidigung erkennbar, insbesondere in Bezug auf vorhandene, eingespielte Prozesse und Know-how im Umgang mit unterschiedlichen Angriffsszenarios.

Von allen Teilnehmern wurde nach den Testübungen hervorgehoben, dass bei der Netzverteidigung ein effizientes Teamwork eine große Rolle spielt und eine Cyber Range ideale Bedingungen bietet, um das Zusammenspiel im Team zu trainieren und entsprechende Koordinations-, Kommunikations- und Entscheidungsprozesse zu überprüfen und zu optimieren. Von den meisten Teilnehmern sind vor den Testübungen die Bedeutung eines effizienten Teamworks unterschätzt bzw. ihre vorhandenen Fähigkeiten überschätzt worden.

Den Bedarf, das eigene Netzwerke in einer Simulationsumgebung nachzubilden, um unter möglichst realistischen Bedingungen trainieren zu können, sahen die Übungsteilnehmer für das Training von grundlegenden Inhalten und Prozessen im Rahmen der Netzverteidigung nicht. Die Nutzung von Standard-Szenarien wurde hierzu als ausreichend angesehen. Um allerdings Übungskünstlichkeiten zu minimieren, sollte eine Reihe unterschiedlicher Standardszenarien verfügbar sein, so dass der Nutzer das Szenario auswählen kann, welches seiner Netzwerkinfrastruktur am nächsten kommt.

Erst für Übungen auf sehr fortgeschrittenem Niveau wurde der Bedarf der Nachbildung nutzerspezifischer Netzwerktopologien gesehen. Insbesondere im Bundeswehrbereich wird dieser Anforderung wesentliche Bedeutung beigemessen, um zum Beispiel auch einsatzvorbereitendes Training durchführen zu können.

Im Rahmen der Nachbildung realer Netzwerke ergibt sich ein Synergieeffekt, der für den Großteil der Übungsteilnehmer relevant war: Unter Nutzung der Replikation des eigenen Netzwerks eröffnet sich die Möglichkeit, mittels Simulation in realistischer und aussagekräftiger Form Tests und Experimente z. B. in Bezug auf Schwachstellen, Notfallverfahren und Optimierung der Schutzmaßnahmen und -technologien vorzunehmen.

Die Möglichkeit der Einbindung von Realkomponenten, wie z. B. unterschiedliche IT-Security-Werkzeuge oder SCADA-Komponenten, ist sowohl für Trainings- als auch Testing-Zwecke von Bedeutung.

Der mögliche hohe Automatisierungsgrad einer Cyber Range und die flexiblen Möglichkeiten, Übungen mit wenig Zeit- und Bedienaufwand durchzuführen, erfüllt vor allem im militärischen Bereich die Forderung nach drillmäßigem Üben.

Zum Schutz sensitiver Nutzerdaten, insbesondere z. B. realer Netzwerkdaten, sind entsprechende Sicherheitsvorkehrungen in einer Cyber Range zu implementieren.

Die Möglichkeit, auf eine Cyber Range über Remote Access zuzugreifen, ist vor allem interessant, wenn sehr wenig Zeit für das Training vorhanden ist und dieses auch nicht gesichert geplant werden kann. Dies trifft zum Beispiel in starkem Maße für CERT- und SOC-Personal zu, deren Verfügbarkeit vom aktuellen Tagesgeschäft abhängig ist. Eine flexible, ortunabhängige Übungsoption kann dieser Anforderung gerecht werden.

4.2 Evaluierung aus Sicht der universitären Lehre

Im Rahmen der Evaluierung fanden mehrere Testübungen mit Studierenden aus den Fachrichtungen Informatik (INF), Wirtschaftsinformatik (WINF) sowie Elektrotechnik und technische Informatik (ETTI) der Universität der Bundeswehr München. Von den insgesamt 25 Studierenden befinden sich 13 in ihrem Bachelor- und 12 in ihrem Master-Studium, sodass in der Evaluation ein breites Spektrum abgedeckt wird. Die Verteilung ist in Abbildung 1 detailliert dargestellt.

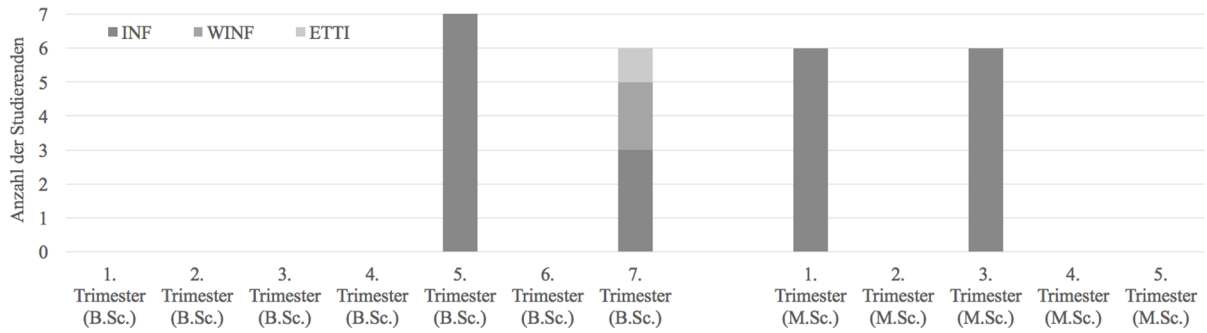

Abb. 1: Verteilung der an der Evaluierung teilnehmenden Studierenden

Im Anschluss an die Testübungen wurden den Studierenden im Rahmen der Evaluierung drei Fragen gestellt:

- Wie ist der Gesamteindruck der Testübungen in der Cyber Range?
- Wie schätzen Sie das Niveau der Aufgaben aus Ihrer persönlichen Sicht ein?
- Halten Sie den Einsatz solch einer Übung im Rahmen der Lehre für zweckmäßig?

Der Gesamteindruck wurde hierbei von allen Teilnehmenden als positiv beschrieben, wobei insbesondere die Möglichkeit praktisch an Systemen zu arbeiten herausgehoben wurde. Hinsichtlich des Niveaus gingen die Wertungen der Studierenden abhängig vom Stand im Studium auseinander. Während die Master-Studierenden das Niveau eher als geeignet einstuften, empfanden die Bachelor-Studierenden es eher als schwierig. Als Grund wurden hierbei das noch nicht vermittelte Wissen im Studium, bzw. noch nicht stattgefundene Praktikumsmodule im Studium angegeben. Die Bedienung der in der Cyber Range verwendeten Tools wurde von einem Teil der Studierenden als schwierig bewertet. Aufgrund mangelnden Wissens ist der Umgang mit den einzelnen Komponenten (z.B. Firewall, Web-Server, Active Directory) als

herausfordernd bewertet. In Abbildung 2 ist veranschaulicht, wie das Niveau der Aufgaben in den Testübungen subjektiv von den Studierenden empfunden wurde. Bezüglich der Zweckmäßigkeit im Rahmen der Lehre waren sich wiederum alle Studierenden einig und beschrieben die Durchführung von Übungen in einer Cyber Range als sehr sinnvoll. Hier wurde nochmals auf die sehr gute Möglichkeit praktische Erfahrungen zu sammeln hingewiesen, da die Möglichkeiten hierfür im Studium gering sind.

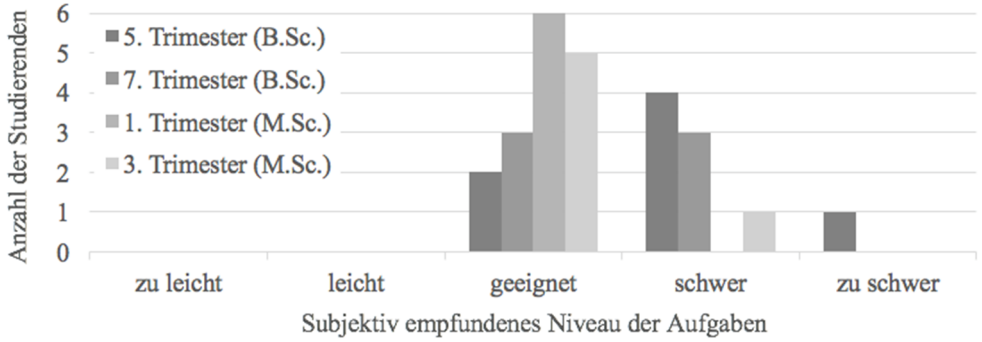

Abb. 2: Subjektiv empfundenes Niveau der Studierenden

5 Kernaussagen und Use Cases

Die Untersuchungen ergaben, dass insbesondere folgende Use Cases einer Cyber Range einen deutlichen Mehrwert für ein Netzverteidigungstraining bieten:

- Eine Cyber Range stellt ein wesentliches Werkzeug im Rahmen der Aus- und Weiterbildung von Fachpersonal dar. Durch den Cyber-Range-Einsatz kann unter Trainer-Anleitung eine deutliche Steigerung der Effizienz der Aus- und Weiterbildung erreicht werden. Komplexe Sachverhalte und Abhängigkeitsverhältnisse können plastisch und somit leicht nachvollziehbar dargestellt werden. Durch einen hohen praktischen Übungsanteil kann die Ausbildungsdauer reduziert werden bzw. die Möglichkeit geschaffen werden, in derselben Zeit höhere Lernziele zu verwirklichen.
- Im Rahmen von simulationsgestützten Übungen können Teams mit den unterschiedlichsten Angriffsvektoren konfrontiert werden. Dabei kommt es darauf an, unter möglichst realistischen Bedingungen – d.h. Realzeit / Zeitdruck, Einsatz von operativen Werkzeugen, Kommunikation im Team – nicht nur die Angriffserkennung zu üben, sondern vor allem die Konsequenzen von Angriffen zu bewältigen. Dazu gehören die Spurensuche im Netz, das Rückgängigmachen von Angreiferaktionen und die Beseitigung von Sicherheitslücken. In derartigen Übungen können Handlungsabläufe, Entscheidungs- und Kommunikationsprozesse sowie die Handhabung von Werkzeugen in die Praxis umgesetzt und optimiert werden. Daneben können Prozesslücken aufgedeckt werden. Im militärischen Umfeld können die Übungsteilnehmer auf spezifische Bedingungen im Einsatzgebiet vorbereitet werden.
- Eine Cyber Range bietet insbesondere die Möglichkeit, verteilte Übungen durchzuführen. D. h. die Übungsteilnehmer befinden sich an unterschiedlichen Orten und loggen sich über eine sichere Remote-Anbindung in den Simulationsserver der Cyber Range ein. Dies eröffnet die Möglichkeit, die Bewältigung von organisationsübergreifenden Cyber-Angriffen im Zusammenwirken unterschiedlicher Teams auf der Basis einer gemeinsamen simulierten Lageentwicklung zu trainieren.

Aus dem Blickwinkel der universitären Lehre bieten Cyber-Simulationssysteme weitere nützliche Use Cases, welche die theoretische Ausbildung um praktische Anteile erweitern können:

- Eine Cyber Range eignet sich hervorragend für die Durchführung von Praktikumsmodulen. Der Schwerpunkt der durchgeführten Übungen kann hierbei auf den Fokus der entsprechenden Lehrveranstaltung gewählt werden. Beispielsweise kann im Rahmen eines Praktikums für Netzsicherheit zunächst die Analyse und Bewertung der gegebenen Infrastruktur im Fokus stehen. Im Gegensatz dazu kann der Schwerpunkt ebenso auf die IT-Forensik gelegt werden, indem die Simulationsumgebung so vorbereitet wird, dass der Angriff bereits stattgefunden hat und entsprechend forensische Erkenntnisse gewonnen werden sollen.
- Ein weiterer Anwendungsfall findet sich im Rahmen vorlesungsbegleitender Übungen. Eine Cyber Range eignet sich hierbei zur Durchführung von kleineren Szenarien, welche den in der theoretischen Vorlesung vermittelten Stoff praktisch anwendbar machen. Ein Fallbeispiel ist die praktische Konfiguration von Firewalls, Routern und anderen Komponenten, welche im Anschluss in der Simulationsumgebung auf einfache Weise überprüft werden können.
- Letztendlich bietet eine Cyber Range ebenso die Möglichkeit die Forschung zu unterstützen. Einerseits können prototypische Implementierungen, welche im Zuge studentischer Abschlussarbeiten entstehen, in eine Cyber Range eingebunden und hinsichtlich des gewünschten Verhaltens überprüft werden. Auf diese Weise wird ein großer Mehrwert für die Forschungsarbeit geschaffen, da innerhalb eines realitätsnahen Systems getestet werden kann. Gleichzeitig wird erreicht, dass eventuell auftretendes Fehlverhalten des Prototyps keine Auswirkungen auf die Infrastruktur außerhalb der Simulationsumgebung hat. Andererseits kann mittels einer Cyber Range das Verhalten von zu untersuchender Hard- und (Schad-)Software analysiert werden. Dadurch können wesentliche Erkenntnisse für Arbeiten erlangt werden, ohne die Infrastruktur außerhalb der Simulationsumgebung zu beeinflussen oder zu schädigen.

Neben dem Training und der Lehre schließt das Cyber-Range-Einsatzspektrum auch Testing & Experimentation ein. Hier sind folgende Use Cases hervorzuheben:

- Durch die Einbindung von IT-Sicherheitskomponenten und -produkten ist es möglich, diese hinsichtlich Funktionalität, Wirksamkeit, Performance, Konfiguration, Bedienbarkeit und Schwachstellen zu prüfen und weiterzuentwickeln. Dies setzt die Verfügbarkeit entsprechender Schnittstellen voraus.
- Operative IT-Netze können anhand einer simulierten / emulierten Nachbildung hinsichtlich Schwachstellen in Bezug auf aktuelle bzw. neue Cyber-Angriffsverfahren untersucht werden.
- Business-Impact-Simulationen erlauben die Untersuchung möglicher Auswirkungen bei Ausnutzung von Schwachstellen durch Angreifer
- Vorhandene oder neue IT-Sicherheitskonzepte bzw. -strategien sowie entsprechende IT-Sicherheitsprozesse und -maßnahmen können in unterschiedlichen Angriffsszenarios überprüft werden.
- Veränderungen von Infrastrukturen und Topologien können getestet werden, IT-Personal kann im Vorfeld der Implementierung der Veränderungen im Rahmen von Trainings vorbereitet werden.

Grundvoraussetzung für Testing & Experimentation-Einsätze ist die Möglichkeit, Simulationen unter reproduzierbaren Bedingungen durchzuführen. Wesentlicher Aspekt hierbei ist die Möglichkeit der Automation der Angriffssimulation.

6 Ausblick

Im universitären Umfeld wird im nächsten Schritt untersucht, wie der Einsatz einer Cyber Range in das Curriculum des Master-Studienganges Cyber-Sicherheit an der Universität der Bundeswehr München eingebracht werden kann. Grundlage dieser Untersuchungen bilden die hier ermittelten Use Cases.

Die ESG hat die konzeptionellen Arbeiten aus operativer Sicht abgeschlossen und baut derzeit eine Cyber Range auf, welche die dargestellten Use Cases erfüllen wird. Dazu wird das Cyber-Range-Produkt, welches während der Evaluierung sowohl von der Universität der Bundeswehr München als auch von ESG die beste Bewertung erhalten hat, als Ausgangsbasis eingesetzt. Zielsetzung ist, den operativen Betrieb bereits im Juli 2017 aufzunehmen und gemeinsam mit der Universität der Bundeswehr München das Anwendungsspektrum und die Funktionalität der Cyber Range sukzessive zu erweitern und im Rahmen gemeinsamer Forschungsprojekte neue Methoden zu untersuchen und zu entwickeln, um reale Netzwerke und aktuelle Angriffsverfahren effizient in die Simulationsumgebung überführen zu können.

Literatur

[BoSB15] K. Boopathi, S. Sreejith, A. Bithin: Learning cyber security through gamification. In: Indian Journal of Science and Technology, 8. Jg., Nr. 7 (2015). S. 642-649.

[CCVT15] P. Čeleda, Jakub Čegan, Jan Vykopal, Daniel Tovarňák: KYPO – A Platform for Cyber Defence Exercises. In STO-MP-MSG-133: M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. Munich (Germany): NATO Science and Technology Organization, 2015.

[CISC17] Cisco Systems Inc.: 2017 Annual Cybersecurity Report [online]. 2017. URL: http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017 [aufgerufen am 08.04.2017].

[CYBE17] CyberBit Commercial Solutions Ltd.: Cyberbit Range [online]. 2017. URL: https://www.cyberbit.net/solutions/cyber-range/ [aufgerufen am 08.04.2017].

[DaMa13] J. Davis, S. Magrath: A Survey of Cyber Ranges and Testbeds. Defence Science and Technology Organisation Edinburgh (Australia) Cyber and Electronic Warfare Div (2013).

[DaCo15] S. K. Damodaran, J. M. Couretas: Cyber Modeling & Simulation for Cyber-Range Events. Proceedings of the Conference on Summer Computer Simulation, Society for Computer Simulation International (2015).

[DaSm15] S. K. Damodaran, K. Smith: CRIS Cyber Range Lexicon Version 1.0. Massachusetts Inst of Tech Lexington Lincoln Lab, 2015.

[ENIS16] European Union Agency for Network and Information Security (ENISA): Cyber Europe [online]. 2016. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme [aufgerufen am 08.04.2017].

[FeTO14] B. Ferguson, A. Tall, D. Olsen: National Cyber Range Overview. In: Military Communications Conference (MILCOM), IEEE (2014), S. 123-128.

[Fish15] E. Fishler: IAI to supply its Cyber Training Center to DNP in Japan [online]. 2015. URL: http://www.iai.co.il/2013/32981-46483-EN/MediaRoom.aspx [aufgerufen am 08.04.2017].

[MaCR15] A. F. A. Machado, F. A. C. R. Costa, J. L. de Rezende: Use of simulation to achieve better results in cyber military training. In: Military Communications Conference (MILCOM), IEEE (2015). S. 1270-1275.

[NATO16] NATO Cooperative Cyber Defence Centre of Excellence: Locked Shields 2016 [online]. 2016. URL: https://ccdcoe.org/locked-shields-2016.html [aufgerufen am 08.04.2017].

[PTCB16] C. Pham, D. Tang, K. Chinen, R. Beuran: CyRIS: a cyber range instantiation system for facilitating security training. In: Proceedings of the Seventh Symposium on Information and Communication Technology, ACM (2016), S. 251-258.

[Wint12] H. Winter: System security assessment using a cyber range. In: 7th International Conference on System Safety, incorporating the Cyber Security Conference, IET (2012).

[YuDo01] W. Yurcik, D. Doss: Different Approaches in the Teaching of Information Systems Security. In: Proceedings of the Information Systems Education Conference (ISECON, 2001).