Realistische Cybersicherheits-Trainings

CYBER RANGES

Bei Cyberattacken müssen Expertinnen und Experten schnell reagieren können.

Die weltweit steigende Zahl an Cybersicherheitsvorfällen macht gut ausgebildete und praxiserprobte Fachkräfte zu gefragten Expertinnen und Experten. Um sich effizient gegen komplexe Angriffe verteidigen zu können, müssen IT-Sicherheitsteams in realistischen Szenarien geschult werden. Cyber Ranges schaffen eine einzigartige Trainingsumgebung, in der eine Vielzahl von Sicherheitsvorfällen und Angriffen simuliert werden kann. Die Cyber Range ICE & T (**I**T **C**ompetence **E**ducation & **T**raining) ist das zentrale Labor am Forschungsinstitut CODE für realitätsnahe Schulungen im Bereich der Cybersicherheit und für das Testen neuer Sicherheitsprodukte.

So erreichen Sie uns

Forschungsinstitut Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Str. 22
81739 München

code@unibw.de
+ 49 89 6004 -7302 oder -7303
www.unibw.de/code

Twitter: @FI_CODE
LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Weitere Informationen

www.unibw.de/code/forschung/zentrallabore/cyber-range

Redaktion: Lisa Scherbaum, Team Cyber Range / FI CODE; Abbildungen: C. Siebold, T. Mittermeier / UniBw M, Pasko Maksim / Shutterstock; Gestaltung: M. Berwanger / Tausendblauwerk, www.tausendblauwerk.de

Universität der Bundeswehr München

ICE T
IT Competence
Education & Training

CYBER RANGE

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

ICE & T Cyber Range

Die Cyber Range IT Competence Education & Training (ICE & T) ist eine umfassende und flexible Lösung für praxisnahe Cybersicherheitstrainings.

Sie bietet eine Plattform für das Erlernen und Vertiefen von Kompetenzen im Bereich Cyber Network Operations mit einem starken Fokus auf Teamwork. ICE & T ermöglicht außerdem die Evaluierung neuer Cybersicherheitsprodukte und -verfahren. Während der Trainings werden defensive und offensive Cybersicherheitsszenarien in einer virtualisierten Umgebung simuliert. Die Teilnehmenden lernen, Angriffe zu analysieren und abzuwehren oder Pentesting-Methoden in realen Szenarien einzusetzen.

Unsere Trainings

- Basic Training: Untersuchen von Cybersicherheitsvorfällen im Team
- Advanced Training: Verbessern der Effizienz eines Teams
- Individual Training: Fokus auf persönliche Bedürfnisse ■

In der virtuellen Umgebung von ICE & T können verschiedene Sicherheitsszenarien simuliert werden.

Teamwork im Fokus: Die Teilnehmenden arbeiten gemeinsam an Analyse und Abwehr von Vorfällen.

Ablauf der Trainings

Am FI CODE setzen wir auf ein realistisches und individuelles Trainingserlebnis.

- **Unsere Trainer weisen** die Teilnehmenden in die Trainingsumgebung und die verwendeten Tools (z. B. Firewall und Security Incident and Event Management System, SIEM) ein.
- Die Ausgangssituation wird vorgestellt: Jedes Szenario hat eine eigene Hintergrundgeschichte.
- Die Teilnehmenden untersuchen die Vorfälle, beheben Störungen und beseitigen die Ursachen, um die Ziele des Szenarios im Team (meist vier bis sechs Personen) zu erreichen.
- Zum Ende der Übung werden Szenario und Leistung des Teams in einer Nachbesprechung diskutiert und ausgewertet.

Die derzeit bei ICE & T verfügbaren Szenarien sind in die Kategorien Cyber Incident & Response Management (CIRM) Level 0–2, Supervisory Control and Data Acquisition (SCADA) und Penetration Testing (PT) unterteilt. Zusätzlich bietet die Cyber Range viele Selbstlernmodule und mehr als 80 Einzelübungen aus neun unterschiedlichen Bereichen der Cybersicherheit. ■

Infrastruktur und Aufbau

ICE & T verfügt über zwei bestens ausgestattete Kursräume für Teams mit bis zu sechs Personen.

Die Trainer analysieren die Übungen und können unterstützend eingreifen.

Der Zugriff auf die Trainingsumgebung erfolgt per Remote-Desktop-Sitzung über Terminalserver. In jedem Kursraum stehen den Teams Whiteboards, TV-Bildschirme und ein Touchboard zur Verfügung. Der Trainerraum ist mit drei Arbeitsplätzen ausgestattet: Mithilfe verschiedener Hard- und Softwarekomponenten können von hier aus die Aktivitäten der Teams und der einzelnen Teilnehmenden beobachtet, analysiert und bewertet werden.

Alle Szenarien werden in virtualisierten Trainingsumgebungen bearbeitet und auf vordefinierten Netztopologien durchgespielt. Die modulare Architektur der Range ermöglicht es, neue Szenarien aus verschiedenen Bereichen der Cybersicherheit einfach zu erstellen und zu implementieren. Weitere Netztopologien, Hardwarekomponenten oder Softwarelösungen können zusätzlich integriert werden. ICE & T befindet sich in permanenter Weiterentwicklung, sodass laufend Funktionen verbessert und ausgebaut werden. ■