



CYBER-ANGRIFFE ERKENNEN UND WIRKSAM BEHEBEN

Entwickeln Sie Ihre IT-Mitarbeiter
zu Cyber-Defence-Experten



Auch die besten präventiven Maßnahmen reichen heute nicht mehr aus, um sich vor Cyber-Angriffen zu schützen. Wie erfolgreich Unternehmen bei der Abwehr sind, hängt einerseits von der Wirksamkeit der eingesetzten Technologien ab, steht und fällt aber mit den Fachkräften, die mit diesen arbeiten.

Denn Cyber-Angriffe zu erkennen sowie schnell und effektiv auf diese zu reagieren, kann nicht jeder IT-Mitarbeiter sofort aus dem Effeff. Und weil genau diese Experten auf dem Arbeitsmarkt extrem rar sind, heißt es, in der eigenen IT-Abteilung die notwendige Expertise aufzubauen. Genau hier setzen die „Incident Detection & Response“-Trainings von Computacenter und ESG/CYOSS an.

TRAINING UNTER REALEN BEDINGUNGEN

Die Trainingsmethodik basiert auf moderner Simulationstechnik, mit deren Hilfe die Teilnehmer das zunächst theoretisch Erlernte direkt in die Praxis umsetzen. Jeder Teilnehmer erhält einen vollständig eingerichteten Simulationsarbeitsplatz, an dem er nicht nur eine eigene Netzwerkumgebung, sondern auch zahlreiche Übungsszenarien und alle Werkzeuge findet, die er für die Aufgabe benötigt. Die Trainings können im ESG-eigenen Cyber Simulation & Training Center (CSTC) in München oder mit Remote-Zugang direkt vom eigenen Schreibtisch aus stattfinden.

WAS WIRD GELERNT?

Das Intensiv-Training baut folgende Fähigkeiten auf:

- Anomalien entdecken, Cyber-Angriffe erkennen und verstehen
- IT-Security-Werkzeuge effizient einsetzen
- Angreiferaktionen im Netzwerk nachverfolgen, isolieren und analysieren
- Maßnahmen zur Wiederherstellung des Normalbetriebs durchführen
- Incidents und Eigenmaßnahmen dokumentieren
- Effiziente Abläufe und Zusammenarbeit im Team

METHODIK

Unter fachlicher Anleitung erfahrener Trainer setzen die Teilnehmer die zuvor erlernten Methoden und Werkzeuge in einer hochrealistischen Simulationsumgebung praktisch ein. Live-Übungen in Realzeit trainieren und optimieren die Zusammenarbeit im Team. Je nach Kenntnissen der Teilnehmer werden auch „Red versus Blue“-Szenarien durchgespielt, um Angreifer- und Verteidigerperspektiven gleichermaßen kennenzulernen. Als Abschlusstest erfolgt am Ende des Kurses eine Cyber-Abwehr-Übung im Team.

AN WEN RICHTET SICH DAS TRAINING?

Das 5-tägige Training richtet sich an IT-Administratoren, angeheendes SOC-/CERT-/CSIRT-Personal und Mitarbeiter in der IT-Sicherheit. Grundlagenkenntnisse in IT-Sicherheit, IT-Organisation und Netzwerkthemen werden vorausgesetzt.



Unternehmen müssen belastbares Cyber-Defence-Wissen aufbauen – am besten sofort. Trainings in realistischen Szenarien leisten hierbei einen wichtigen Beitrag.

**Dr. Sebastian Schmerl,
Solution Manager for Cyber
Defense & Industrial Security**



TRAINER

Die Trainingsteilnehmer profitieren vom umfassenden Praxiswissen der Trainer: So bringen die Computacenter Consultants ihr Wissen über reale Angriffsszenarien ein, zu erprobten Maßnahmen zur Detektion und Reaktion sowie zu allen Fragen rund um ein Security Operation Center (Aufbau, Betrieb und Weiterentwicklung sowie Schulung des Personals). Ergänzt wird dies durch ihre langjährige Erfahrung in der Beratung und Umsetzung ganzheitlicher Security-Projekte. Gleichsam unterstützen die Trainer der ESG/CYOSS als Berater seit vielen Jahren ihre Kunden dabei, die Informationssicherheit im Unternehmen nachhaltig zu verbessern – mit maßgeschneiderter Beratung und Umsetzung sowie Training und Testing im CSTC.

WEITERE INFORMATIONEN

