Cyber Incident Games

Schlüpfen Sie in die Rolle eines Cyber Angreifers und planen Sie Ihre eigene Cyber Attacke

Cyber Incident Games sind Trainings für Ihre Mitarbeiter, die IT / OT bisher nur als Anwender wahrnehmen und einsetzen.

Die Teilnehmer schlüpfen im Planspiel in die Rolle eines Cyber Angreifers, erhalten Missionen und planen Cyber Angriffe, die die IT-Infrastruktur im Spiel beeinträchtigen.

Die Cyber Incident Games bieten hier je nach Bedarf des Kunden unterschiedliche IT-Infrastrukturen. Ein klassisches Business-Netzwerk mit Notebooks, stationären Arbeitsplätzen, einem Webautritt u.a. Elementen bietet hier Angriffsflächen für Diebstähle, Phishing-Versuchen oder andere hinterlistige Pläne. Ebenso ist ein Spielplan mit einer industriellen Infrastruktur verfügbar, welcher neben Produktionsanlagen auch wichtige Produktionsdaten enthält.

Wie die Teilnehmer ihre Angriffsmission erreichen und welche Angriffsmethoden sie einsetzen werden ist offen. So können bspw. Methoden des Social Engineerings, schädliche USB-Sticks oder E-Mailanhänge eingesetzt und natürlich auch miteinander kombiniert werden.

Der kriminellen Phantasie und dem Spielspaß sind keine Grenzen gesetzt: Es gewinnt, wer den hinterlistigsten Cyber Angriff entwickelt und die Mission erfolgreich erfüllt.

AIRBUS

Cyber Incident Games

Schlüpfen Sie in die Rolle eines Cyber Angreifers und planen Sie Ihre eigene Cyber Attackes

Im Anschluss an die Planung der Cyber Angriffe werden die verwendeten Angriffstechniken analysiert und IT-Sicherheitsmaßnahmen zur Abwehr diskutiert. Hierbei spielen die vier Dimensionen des BSI (Bundesamt für Sicherheit in der Informationstechnik) Personal, Technik, Organisation und Infrastruktur eine besondere Rolle.

Die Teilnehmer werden durch diese Perspektivenwechsel Angreifer / Verteidiger in realitätsnahe Situationen versetzt, um Schwachstellen, Risiken und Möglichkeiten für Angreifer besser wahrzunehmen. Diese Wahrnehmung wiederum führt zu einem schnelleren Einleiten von Sicherheitsmaßnahmen und natürlich auch zur Akzeptanz von (aus Anwendersicht vielleicht eher hinderlichen) Maßnahmen.

Die Cyber Incident Games werden als IT- / OT-Security Awareness Maßnahme eingesetzt und fördern die Zieldimensionen Wahrnehmung, Wissen und sicherheitskonformes Verhalten. Um diesen Effekt zusätzlich zu steigern sind die Cyber Incident Games mit anderen Airbus IT- / OT-Security Awareness Maßnahmen kombinierbar. Zum Beispiel könnte ein vorangestellter Live-Hacking Vortrag den Teilnehmern zusätzliche Inspiration für ihre eigenen Cyber Angriffe und Schutzmaßnahmen liefern.

In welchem Umfang und Bereich wollen Sie mit uns Cyber Incident Games bei Ihnen durchführen?

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com