Kaspersky Industrial CyberSecurity Trainings und Awareness-Programme

https://www.kaspersky.de/enterprise-security/industrial

#truecybersecurity

Kaspersky Industrial Cybersecurity Trainings und Awareness-Programme

Unser gesamtes Wissen, unsere Erfahrung und unsere Erkenntnisse im Bereich der industriellen Cybersicherheit sind die Grundlage unseres innovativen Schulungsprogramms.

Für rund 80 Prozent aller Cybersicherheitsvorfälle sind Fehler von Mitarbeitern verantwortlich. Wenn diese Vorfälle zu einem Zusammenbruch wichtiger Systeme führen oder den Stopp industrieller Prozesse bedeuten, werden solche Fehler schnell teuer und können sogar das gesamte Unternehmen bedrohen.

In Zeiten, in denen die Bedrohungslandschaft sich stetig weiterentwickelt und gezielte Angriffe vermehrt auf menschliche Schwächen setzen, sind Mitarbeiter, die automatisch und instinktiv die richtigen Sicherheitspraktiken verfolgen, einer der wichtigsten Verteidigungsmechanismen.

Hierzu müssen sich alle Ihre Mitarbeiter der potentiellen Gefahren bewusst sein und wissen, wie sie dennoch sicher arbeiten können. Auch Personal, das direkt für die Cybersicherheit im IT-/OT-Bereich verantwortlich ist, muss über die Fähigkeiten verfügen, die für ein effektives Bedrohungsmanagement sowie für die effektive Erkennung und Abwehr von Angriffen erforderlich sind.

Die Kaspersky Industrial CyberSecurity Trainings und Awareness-Kurse wurden speziell dazu entwickelt, Betreiber kritischer Infrastrukturen, Versorgungsdienstleister und Produktionsunternehmen dabei zu unterstützen, ihre industriellen Umgebungen vor Ausfällen und Schäden durch Cyberbedrohungen und -angriffe zu schützen.

Die Kurse (Sämtliche Schulungen werden in englischer Sprache angeboten.)

<table>
<tr><th>CyberSecurity Awareness</th><th colspan="2">CyberSecurity Skills Development und Trainings</th></tr>
<tr><td>Für Techniker/Mitarbeiter im Industriebereich:</td><td>Für IT-/OT-Experten:</td><td>Für IT-/OT-Sicherheitsexperten:</td></tr>
<tr><td>Basic Cybersafety</td><td rowspan="3">Advanced Industrial CyberSecurity in Practice</td><td>ICS Penetration Testing for Professionals</td></tr>
<tr><td>Für Führungspersonal:</td><td rowspan="2">ICS Digital Forensics for Professionals</td></tr>
<tr><td>Industrial Cybersafety Games</td></tr>
</table>

Industrial Cybersecurity Awareness

Diese Kurse umfassen interaktive Online- und Vor-Ort-Schulungsmodule und Simulationsspiele rund um die Cybersicherheit für alle Mitarbeiter, die in der Produktion, im Kontrollraum oder im Back-Office mit industriellen Computersystemen arbeiten, sowie für ihre Vorgesetzten.

Unternehmen geben Millionenbeträge für Schulungen zur Cybersicherheit aus, aber nur wenige CISOs sind mit den Ergebnissen wirklich zufrieden. Woran liegt das?
Die meisten Schulungen zur Schärfung des Bewusstseins für Cybersicherheit gehen nicht genug ins Detail und sind darüber hinaus zu lang, zu technisch und allgemein negativ gehalten. Sie schulen nicht die wichtigsten Bereiche, nämlich die Entscheidungsfindung und die Lernfähigkeit der Teilnehmer, was häufig dazu führt, dass die Schulungen keine Wirkung zeigen. Darüber hinaus spiegeln sie nicht die Herausforderungen wider, denen sich Mitarbeiter im industriellen Bereich ausgesetzt sehen.

Unternehmen sind deshalb an differenzierteren Methoden und Ansätzen für die Verhaltensschulung interessiert (wie z. B. die Förderung der Unternehmenskultur), die sich auf Probleme konzentrieren, die für ihre eigene Arbeitsumgebung spezifisch sind, und eine messbare Rendite erzielen.

Die Industrial Cybersecurity Awareness-Kurse von Kaspersky Lab beruhen auf den folgenden Grundprinzipien:

- Änderung des Verhaltens, sodass Mitarbeiter bemüht sind, sicher und verantwortungsbewusst zu arbeiten, und eine gemeinsame Umgebung schaffen, in der sich alle um die Cybersicherheit kümmern – weil es einfach zur Tätigkeit dazugehört.
- Kombination aus Motivation, Planspielen, Angriffssimulationen basierend auf industriellen Situationen aus dem echten Leben und interaktiven Schulungen zum Erlernen umfassender Kompetenzen im Bereich der Cybersicherheit.

So funktionieren die Kurse im Detail

Umfassend, aber verständlich: Die Schulungen decken über eine Reihe einfach aufgebauter Übungen eine breite Palette unterschiedlicher Sicherheitsaspekte ab: von simplen Sicherheitsregeln, über Malware-Angriffe und Datenlecks bis hin zum sicheren Umgang mit Sozialen Netzwerken. Wir nutzen verschiedene Lehrmethoden, wie z. B. Gruppenarbeit, interaktive Module und Planspiele basierend auf Szenarien aus dem industriellen Alltag, um die Teilnehmer anzusprechen und ihnen relevante Inhalte zu vermitteln.

Verfügbar: Unser eintägiger Kurs „Cybersafety Awareness" kann direkt im Unternehmen oder an einem beliebigen anderen Veranstaltungsort angeboten werden, während Kaspersky Industrial Protection Simulation (KIPS), unser spielerisches Industrial Cybersecurity-Programm, online oder gegen andere Teilnehmer gespielt werden kann. Um eine realistische Lernumgebung zu schaffen, stehen unterschiedliche KIPS-Varianten für verschiedene Branchen, wie z. B. Wasseraufbereitung oder Energieversorgung und -übertragung, zur Verfügung.

Kontinuierliche Motivation: Wir erreichen über Spiel- und Konkurrenzsituationen Lernmomente, die im Laufe des Jahres durch simulierte Angriffsübungen sowie Assessment- und Schulungsinitiativen verstärkt werden.

Verändertes Sicherheitsbewusstsein: Mitarbeiter lernen die Bedeutung ihrer eigenen Rolle beim Schutz vor spezifischen Bedrohungen kennen und erfahren, wie sie es vermeiden können, selbst zum Opfer eines Angriffs zu werden und sich und ihren Arbeitsplatz den Gefahren eines Angriffs auszusetzen.

Unternehmensweite Cybersicherheitskultur: Wir bringen Führungskräften bei, als Botschafter für Sicherheit aufzutreten, denn eine Unternehmenskultur, in der Cybersicherheit allen selbstverständlich ist, lässt sich nicht einfach durch die IT-Abteilung vorschreiben – sie lässt sich am besten durch das Engagement und gute Vorbild von Vorgesetzten realisieren.

Positive Bestärkung und Zusammenarbeit: Wir demonstrieren den positiven Einfluss, den Sicherheitspraktiken auf die allgemeine betriebliche Effizienz und Produktivität haben, und setzen uns für die effektive Zusammenarbeit mit anderen internen Abteilungen ein, unter ihnen auch das IT-/OT-Sicherheitsteam.

Messbarkeit: Wir stellen Hilfsmittel zur Messung der Mitarbeiterkompetenz bereit sowie unternehmensweite Assessments zur Analyse der Mitarbeitereinstellung zur Cybersicherheit im Arbeitsalltag.

Cybersecurity Skills Development und Trainings

Diese Kurse decken ein breites Spektrum verschiedener Themen rund um die Cybersicherheit ab und vermitteln Mitarbeitern, die heute oder in Zukunft direkt mit der Sicherheit industrieller Systeme und Technologien betraut sind, die richtigen Techniken. Alle Kurse werden am Kundenstandort oder, sofern erwünscht, in einer lokalen oder regionalen Niederlassung von Kaspersky Lab angeboten.

Die Teilnehmer arbeiten und lernen zusammen mit unseren globalen Experten, die sie durch ihre eigene Erfahrung im alltäglichen Kampf bei der Vorhersage, dem Verhindern und Erkennen sowie der Abwehr von Cyberbedrohungen inspirieren.

Die Kurse umfassen sowohl theoretische Lektionen als auch praktische Übungen. Nach Abschluss jedes Kurses können die Teilnehmer ihr Wissen in einem Test prüfen.

Mehr Fachwissen für Ihr Unternehmen

Diese Schulungskurse ermöglichen es Unternehmen, das gesammelte Wissen zur Cybersicherheit in drei Hauptbereichen zu erweitern:

- Grundlegendes Wissen zur Cybersicherheit industrieller Kontrollsysteme
- ICS-Penetrationstests
- Digitale Forensik für ICS

Advanced Industrial CyberSecurity in Practice

In dieser Schulung erhalten Ihre IT-/OT-Experten neue Einblicke in die derzeitige Bedrohungslandschaft, erfahren, welche Angriffsvektoren aktuell für Ihre Branche eingesetzt werden, und erlangen alle erforderlichen Fertigkeiten zum Aufbau eines grundlegenden Vorfallsreaktionsplans.

ICS Penetration Testing for Professionals

Dieser Kurs ermöglicht es IT-/OT-Sicherheitsexperten, umfassende und gründliche Penetrationstests in industriellen Umgebungen durchzuführen und geeignete Behebungsmaßnahmen zu empfehlen.

ICS Digital Forensics for Professionals

Dieser Kurs ermöglicht es IT-/OT-Sicherheitsexperten, erfolgreiche forensische Untersuchungen und Analysen in industriellen Umgebungen durchzuführen und entsprechende Empfehlungen zu geben.

Die Kurse im Detail

Themen	Dauer	Ergebnis/Erlernte Fertigkeiten
Advanced Industrial CyberSecurity in Practice		
• Überblick zur aktuellen Bedrohungslandschaft, zu Sicherheitsproblemen, zum Faktor Mensch und zu ICS-Netzwerkangriffen • Besonderheiten der Netzwerksicherheit in IT- und ICS-Umgebungen • Fallstudie, die den Einsatz von Vermeidungs-, Erkennungs- und Abwehrtechnologien zeigt • Compliance mit Industriestandards und Gesetzgebung • Netzwerktopologien und Funktionsweise von Sicherheitstechnologien • Cybersicherheitsrollen und Teamstrukturen • Allgemeine Fehler bezüglich der Sicherheit	1 bis 2 Tage	• Verstehen aktueller industrieller Cyberbedrohungen und Bekämpfen von Vorfällen in Ihrer Branche/ Ihrem Unternehmen • Erkennen von Sicherheitsvorfällen • Ausführung von grundlegenden Untersuchungen • Planen und Implementieren eines effektiven Vorfallsreaktionsplans Dieser Kurs umfasst individuell anpassbare Elemente und kann in einem oder zwei Tagen abgeschlossen werden. Führt zu Zertifizierung.
ICS Penetration Testing for Professionals		
• Einführung in die ICS-Komponenten, die -Architektur und das -Deployment in verschiedenen Branchen: – Energieversorgung – Öl und Gas – Transport • Praxisnahe Techniken für Penetrationstests in diesen und anderen ICS-Umgebungen • Erstellen eines ICS-Penetrationstestplans samt Überlegungen und Einschränkungen • Informationsbeschaffung • Schwachstellenanalyse bei SCADA- und PLC-Systemen • Ergebnisanalyse und Reporting • Praxisübungen	5 Tage	• Verstehen und Analysieren der Schwachstellen in industriellen Kontrollsystemen • Erstellen eines effektiven ICS-Penetrationstestplans • Durchführen sicherer und erfolgreicher Penetrationstests in SCADA- und PLC-Systemen und anderen Elementen von ICS • Empfehlen geeigneter Behebungsmaßnahmen Führt zu Zertifizierung.
ICS Digital Forensics for Professionals		
• Einführung in die ICS-Komponenten, die -Architektur und das -Deployment in verschiedenen Branchen: – Energieversorgung – Öl und Gas – Transport • Anerkennen und Arbeiten mit den Herausforderungen und Einschränkungen von ICS • Digitale forensische Techniken in ICS-Umgebungen • Erstellen eines Plans für die digitale Forensik in ICS • Manuelles Erfassen und Aufbewahren forensischer Daten und Arbeit mit RTOS- und ICS-Protokollen • Analyse von Artefakten und Anomalienüberprüfung • Reporting • Praxisübungen	4 Tage	• Durchführen erfolgreicher forensischer Untersuchungen in ICS-Umgebungen • Erstellen eines effektiven Plans für die digitale Forensik in ICS • Sammeln und ordnungsgemäße Handhabung physischer und digitaler Beweise • Anwenden der Werkzeuge und Instrumente der digitalen Forensik auf SCADA und PLC • Finden der Spuren von Eindringversuchen basierend auf Artefakten • Rekonstruktion von Vorfällen und Verwendung von Zeitstempeln • Bereitstellen umfassender Informationen und Empfehlen geeigneter Aktionen Führt zu Zertifizierung.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity ist ein Portfolio bestehend aus Technologien und Services, das umfassenden Schutz für jede einzelne Ebene von Betriebstechnologie und sämtliche Elemente Ihres Unternehmens bietet, darunter auch für SCADA-Server, HMIs, Engineering-Workstations, SPS, Netzwerkverbindungen und Mitarbeiter, ohne dabei die Geschäftskontinuität und Konsistenz der technologischen Prozesse zu beeinträchtigen.

Weitere Informationen zu Kaspersky Lab finden Sie unter
https://www.kaspersky.de/enterprise-security/industrial

Informationen über ICS Cybersicherheit:
https://ics-cert.kaspersky.com
Neues über Cyberbedrohungen: **www.viruslist.de**

#truecybersecurity

www.kaspersky.de

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* Auszeichnung für weltweit führende Leistungen in den Bereichen Internetwissenschaft und Internettechnologie auf der 3. Weltinternetkonferenz (Wuzhen-Gipfel)
** Sonderpreis der Industriemesse China International Industry Fair (CIIF) 2016