Live Hacking: Praxisbeispiele für Angriffe auf kritische Infrastrukturen

(Mögliche) Titel
Live Hacking Industrial Control Systems (ICS) – Angriffsszenarien auf kritische Infrastrukturen
„Houston. Wir haben ein Problem!" - Angriffsszenarien auf kritische Infrastrukturen
Live Hacking Industrial Control Systems (ICS) – Angriff am Fließband
Die Entführung der U-Bahn Pelham 123 – ein Praxisbeispiel für Angriffe auf kritische Infrastrukturen
Gefahr in (Ver)Zug! – Praxisbeispiele für Angriffe auf kritische Infrastrukturen
Gefahr in (Ver)Zug! – Praxisbeispiele für Angriffe im Internet der Dinge (IoT – Internet of Things)
Live Hacking 4.0 – Sicherheitsrisiken von Industrie 4.0 und IoT verstehen
Live Hacking 4.0 – Industrie 4.0 und IoT: Im Land der unbegrenzten Möglichkeiten

Inhalt
Nach dem Megatrend Cloud Computing werden Industrie 4.0 und Internet der Dinge (IoT) abermals die bestehenden IT-Konzepte und -Prozesse in den Unternehmen verändern.

Durch das „Verheiraten" der Produktion mit der klassischen IT können Hacker-Angriffe drastische Folgen haben. Hackerangriffe und Cyber-Spionage auf kritische Infrastrukturen sind deshalb zu einer ständigen Bedrohung der industriellen IT geworden. Trojaner und Malware werden speziell dazu entwickelt, Produktions- und Versorgungsanlagen gezielt zu sabotieren oder Informationen über industrielle Steuerungsanlagen und Systeme zu sammeln. Dabei stehen Industriestaaten ganz besonders im Fokus.

„Aber kritische Infrastrukturen unterliegen doch strengen Sicherheitsvorgaben. Ein Angriff kann daher bestimmt nicht so einfach sein, oder?"

Leider doch! Neben hochkomplexen Cyberwaffen stellen insbesondere bekannte IT-Sicherheitslücken ein Risiko für Unternehmen und deren Produktionsanlagen dar. Die Vielfalt der Angriffsmöglichkeiten eröffnet eine neue Gefahrendimension. Der Verlust wichtiger Unternehmensdaten und schützenswerter Informationen ist schwerwiegend – wird jedoch gegenüber der Gefahr des Produktionsstillstands oder der Beeinflussung der Abläufe häufig als das „geringere Problem" betrachtet. Jeder erfolgreiche Angriff auf die industrielle IT bedeutet auch eine Bedrohung für Mensch und Umwelt!

Methodik

In Fallbeispielen wird konkret aufgezeigt, welche Methoden Cyberkriminelle verwenden, um Produktions- und Steuerungsprozesse zu attackieren. Die Methoden werden theoretisch erläutert und live demonstriert.

Dem Auditorium werden die Inhalte anschaulich, unterhaltsam und vor allem nachhaltig vermittelt. Zudem wird im Vortrag auf aktuelle Themen und Inhalte eingegangen.

Zielgruppe
Der Vortrag richtet sich an Elektro-, Automatisierungs- und Prozessverfahrenstechniker bzw. Ingenieure, die sich mit dem Betrieb und der Administration von Automatisierungstechnik auseinandersetzen. Ebenso sind technische Entscheidungsträger und leitende Angestellte eingeladen, die die industrielle IT und deren Sicherheit besser verstehen bzw. kennenlernen wollen.

Voraussetzungen:	Basiskenntnisse (industrielle) IT, Automatisierungstechnik
Schwierigkeitsgrad:	leicht bis mittel

Eine zielgruppengerechte Präsentation und Keynote Speech ist ebenfalls möglich.

Dauer
60 Minuten. Ein individueller und formatgerechter Zeitrahmen von 30 bis 180 Minuten ist ebenfalls möglich (vom erfrischenden Impulsvortrag bis hin zur abendfüllenden Veranstaltung).

Referent
Vita (lang)
Marco Di Filippo ist seit seiner Kindheit ein Computer-Enthusiast. Seinen ersten Arbeitsschwerpunkt legte er auf das Konfigurieren und Projektieren von Kommunikationshardware. Danach konzentrierte er sich auf das Programmieren von industriellen Steuerungssystemen im Bereich der Automatisierung und Informationstechnologie.

Er arbeitet seit 1996 im IT-Consulting, davon mehr als 15 Jahre im Bereich IT-Sicherheit, sowohl aus der offensiven als auch aus der defensiven Sicht. Sein Spezialgebiet sind organisatorische und technische IT-Sicherheitsprüfungen und -konzepte. Er ist in leitender Position bei der KORAMIS GmbH, Saarbrücken tätig.

Schon lange vor Bekanntwerden von Cyber-Angriffen warnte Herr Di Filippo die Öffentlichkeit vor unzureichend abgesicherten industriellen Steuerungssystemen (ICS – Industrial Control Systems). Er war somit maßgeblich an der Sensibilisierung

für mögliche Cyber-Bedrohungen und an der Verbreitung entsprechender Cyber-Security-Strategien beteiligt.

Herr Di Filippo verfügt über langjährige, praktische Projektleitungs- und Beratungserfahrung in verschiedenen Branchen. Zusätzlich ist er als Referent an Universitäten und Fachhochschulen, bei Fachveranstaltungen, auf Messen sowie bei Schulungen und Workshops aktiv. Durch seine locker-lässige Art vermittelt er den Zuhörern die IT-Sicherheit anschaulich, unterhaltsam und vor allem nachhaltig. Er ist zudem Autor zahlreicher Publikationen und Mitautor diverser Fachbücher. In der Fachpresse und in seinem Blog publiziert Herr Di Filippo regelmäßig über die rasanten Entwicklungen bezüglich Sicherheitslücken und -vorfällen sowie neuste (Forschungs-)Erkenntnisse der Branche.

Vita (mittel)
Marco Di Filippo ist seit seiner Kindheit ein Computer-Enthusiast und arbeitet seit 1996 im IT-Consulting, davon mehr als 15 Jahre im Bereich IT-Sicherheit, sowohl aus der offensiven als auch aus der defensiven Sicht. Sein Spezialgebiet sind organisatorische und technische IT-Sicherheitsprüfungen und -konzepte. Er ist in leitender Position bei der KORAMIS GmbH, Saarbrücken tätig.
Schon lange vor Bekanntwerden von Cyber-Angriffen warnte Herr Di Filippo die Öffentlichkeit vor unzureichend abgesicherten industriellen Steuerungssystemen (ICS – Industrial Control Systems). Er war somit maßgeblich an der Sensibilisierung für mögliche Cyber-Bedrohungen und an der Verbreitung entsprechender Cyber-Security-Strategien beteiligt.

Herr Di Filippo ist Autor zahlreicher Publikationen und Mitautor diverser Fachbücher. In der Fachpresse und in seinem Blog publiziert er regelmäßig über Sicherheitslücken und -Vorfälle sowie neuste (Forschungs-)Erkenntnisse der Branche.

Vita (kurz)
Marco Di Filippo ist seit seiner Kindheit ein Computer-Enthusiast. Er ist Autor, Blogger, Berater und hält Fach- und Publikumsvorträge. Sein Spezialgebiet sind organisatorische und technische IT-Sicherheitsprüfungen und -konzepte.