Live Hacking: Praxisbeispiele für Angriffe im Internet der Dinge (IoT)

(Mögliche) Vortragstitel
Licht aus, Vorhang auf, Bühne frei! Smart-Home-Hacking
Sicherheitsrisiko Smart Home – Der Hacker kommt durch den Kühlschrank
Sicherheitsrisiko IoT – Der Hacker kommt durch den Kühlschrank
Sicherheitsrisiko Smart Home – Der Einbrecher kam aus dem Internet

Inhalt
Hackerangriffe im Internet der Dinge (englisch Internet of Things, Kurzform: IoT) auf intelligente Gebäudesteuerungen (Smart Homes) sind zu einer realen Bedrohung geworden. Immer mehr Alltagsgeräte bekommen Internet-Zugang. Eine Studie zeigt: Das vernetzte Haus hat teils massive Sicherheitslücken. Sie werden zum Einfallstor für Hacker.

Per App Lampen zu steuern, ist nur eine von immer mehr Optionen. Schon öffnen sich Rollladen, sobald die Sonne aufgeht; die Uhrzeit liefert das Web. Thermometer lernen, wann die Bewohner zu Hause sind – und regeln die Heizung. Bewegungsmelder warnen übers Handy, wenn sich daheim Ungewöhnliches tut. Fenster und Türen schicken SMS, wenn jemand sie öffnet.

Ein Angriff auf Smart Homes betrifft mich nicht. Oder doch?

Leider schon! Neben komplexen Cyberwaffen stellen insbesondere bekannte IT-Sicherheitslücken ein Risiko für Endverbraucher dar. Die Vielfalt der Angriffsmöglichkeiten eröffnet eine neue Gefahrendimension, denn mit steigender Vernetzung nehmen der Einsatz und der Einfluss der IT im Internet der Dinge zu. Teils nutzten Hersteller nicht die etablierten Standards zur Verschlüsselung der Verbindung. Oder Benutzer müssen sich nicht authentifizieren, wenn sie auf steuerbare Objekte zugreifen. Und selbst wenn das bei der Fernsteuerung übers Internet vorgesehen ist, wird das Passwort oftmals unverschlüsselt gesendet. Dabei kann von einem erfolgreichen Angriff auf die Smart-Home-Technik eine Bedrohung für Mensch und Umwelt ausgehen.

Methodik
In Fallbeispielen wird konkret aufgezeigt, welche Methoden Angreifer verwenden, um Geräte im Internet der Dinge 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 Inhalten eingegangen.

Zielgruppe
Der Vortrag richtet sich an Elektro-, Automatisierungs- und Prozessverfahrenstechniker bzw. Ingenieure, die sich mit dem Betrieb und der Administration von Gebäudetechnik auseinandersetzen. Ebenso sind Anwender eingeladen, die das IoT und dessen (Un-)Sicherheit besser verstehen bzw. kennenlernen wollen.

Voraussetzungen:	Basiskenntnisse IT, Gebäudetechnik
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.