Live Hacking: Praxisbeispiele für Angriffe auf mobile Endgeräte

(Möglicher) Vortragstitel
Live Hacking Mobile Security – Angriffsszenarien auf mobile Dienste
Live Hacking Mobile Security – Angriffsszenarien auf mobile Endgeräte
Wie (un-)sicher sind iPhone, Android & Co.?
Max Schmitt – denn er weiß nicht, was er tut!
Max Schmitt unterwegs – Angriffsfläche mobile Endgeräte

Inhalt
Viele Anwender wissen nicht über die Sicherheitsrisiken ihrer ständigen Begleiter Bescheid. So mancher ignoriert diese Problematik sogar bewusst! Die Enthüllungen der Spähaktion von NSA & Co. haben gezeigt, dass Science Fiction à la James Bond bereits Realität ist.

Mobile Security – warum? Betrifft mich das? Bin ich so wichtig? Das wird doch nicht ausgerechnet mich treffen …

Die Realität zeigt, dass jeder betroffen sein kann, vom einfachen Bürger bis hin zum Spitzenpolitiker.

Laptop, iPhone, Android & Co. sind heute und morgen die Kommunikationsmittel, die uns überall begleiten und dabei oft offen wie Scheunentore sind. Ohne Mobiltelefon fühlt man sich nicht komplett. Die Funktionsvielfalt der Smartphones nimmt rasant zu, wobei die Möglichkeiten fast unbegrenzt sind.
Was vertrauen wir ihnen nicht alles an: Kontaktdaten, Termine, vertrauliche Nachrichten, (persönliche) Bilder, Zugangsdaten für Konten usw. Jeder, der ein wenig technischen Sachverstand mitbringt, kann den Standort des Handys ermitteln, fremde SMS-Nachrichten lesen, es als Gateway benutzen und sogar Gespräche belauschen.

Methodik
Anhand diverser Szenarien, wie zum Beispiel SAT (SIM Application Toolkits), Early-Media-Angriffe (Freizeichentöne), Call- und SMS-ID-Spoofing, Mitlauschen von Gesprächen und Daten (SMS, E-Mail), Ortung, Malware, Bluetooth- und WLAN-Hacking, werden im Workshop/Vortrag verschiedene Angriffsszenarien erläutert und live demonstriert. Ergänzt werden diese durch Erfahrungsberichte aus verschiedenen Feldversuchen.

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

Zielgruppe
Der Workshop richtet sich an technische Entscheidungsträger und leitende Angestellte, die sich mit der Anwendung, Administration und Einführung von mobilen Diensten im Unternehmen auseinandersetzen. Ebenso sind Anwender und Mitarbeiter eingeladen, die die technischen Zusammenhänge mobiler Dienste besser verstehen bzw. kennenlernen wollen.

Voraussetzungen:	Basiskenntnisse Mobile Networks von Vorteil
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.