



## **Live Hacking: Das private Umfeld als Angriffsziel für Wirtschafts- und Industriespionage**

### **(Möglicher) Vortragstitel**

Max Schmitt – denn er weiß nicht, was er tut!

Max Schmitt zu Hause – der fließende Übergang zwischen beruflichen und privaten Daten

### **Inhalt**

Notebook, Smartphone und Tablet sind für viele Nutzer kaum noch aus dem Alltag wegzudenken und bewähren sich als ständige Begleiter für Freizeit und Beruf. Die Generation der „Digital Natives“ drängt in die Arbeitswelt – und bringt ihre modernen Notebooks, Tablets und Smartphones gleich mit. Damit neigen sich die Zeiten dem Ende zu, in denen nur privilegierte Mitarbeiter Zugriff von unterwegs auf das geschäftliche Kommunikationsgeschehen und Unternehmensdaten erhielten. Als Aushängeschild für moderne Unternehmenskultur gehört der Einsatz privater Geräte im Unternehmen (BYOD: bring your own device) inzwischen zum guten Ton.

Oft wird dabei vergessen, dass jeder Mensch neben seiner beruflichen Seite auch ein privates Leben hat. Gerade im privaten Umfeld verlieren viele User ihre Sensibilität für Datensicherheit. Ich bin doch nicht so wichtig. Alles nicht so schlimm. Meine Daten interessieren niemanden. Behauptungen wie diese sind gerade im privaten Umfeld alltäglich.

Doch wo fängt die Privatnutzung an und hört die geschäftliche Nutzung auf? Wo sind die Grenzen in der Infrastruktur? Wer hat sonst noch Zugriff auf die Geräte? Wie wird der Kalender zwischen privat und geschäftlich getrennt? Wie ist das heimische WLAN abgesichert? Wenn die Grenzen zwischen Beruflichem und Privatem zu sehr verschwimmen, kann das die Vertraulichkeit, Integrität und Authentizität der Unternehmensdaten gefährden.

Auch Cyberkriminelle haben erkannt, dass das private Umfeld nur unzureichend auf Hackerangriffe, Datendiebstahl und andere Formen von Cyberkriminalität vorbereitet ist. Diese Tatsache wird ausgenutzt, um über die heimische Infrastruktur an vertrauliche Unternehmensdaten zu gelangen.

### **Methodik**

Der Vortrag bietet einen Einblick in die Gefahren, die in Verhaltensweisen und im Umgang mit Unternehmensdaten im heimischen Umfeld lauern. Anhand eines fiktiven Opfers (Max Schmitt) werden diese erläutert und live demonstriert. Ergänzend hierzu werden Beispiele aus der Praxis gezeigt.



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. Ebenso sind Anwender und Mitarbeiter eingeladen, die Notebook, Smartphone, Tablet usw. sowohl privat als auch geschäftlich nutzen.

Voraussetzungen:

IT-Basiskenntnisse 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.