Live Hacking: Von klassischen Viren bis zur komplexen Malware

(Mögliche) Vortragstitel
Max Schmitt – Befallen von Viren, Würmern, Trojanern, Ransomware und anderem digitalen Ungeziefer
Max Schmitt infiziert– Von klassischen Viren bis zur komplexen Malware
Max Schmitt infiziert – Viren, Würmer, Trojaner, Ransomware und weiteres digitales Ungeziefer, das Handwerkszeug von Cyberkriminellen
Max Schmitt – auch er ist erpressbar... Ransomware erkennen und abwehren
Malware Attack – Viren, Würmer, Trojaner, Ransomware und Co. genau erklärt
LiveHacking – Viren, Würmer, Trojaner, Ransomware und weiteres digitales Ungeziefer, das Handwerkszeug von Cyberkriminellen
Malware-Infektion – Viren, Würmern, Trojanern, Ransomware und anderem digitalen Ungeziefer auf den Zahn gefühlt

Inhalt
Wenn man heute über Schadprogramme oder Malware spricht, so ist damit eine große Familie von Computerprogrammen gemeint, die entwickelt wurden, um gegen den Willen des Eigentümers schädliche Aktionen auf Computern durchzuführen. Es gibt mittlerweile zahlreiche Unterarten von Malware, zum Beispiel Viren, Trojaner, Rootkits, Ransomware oder Spyware. Alle arbeiten anders und haben unterschiedliche Aufgaben. Ihre Schöpfer haben mittlerweile wahre „Meisterwerke" an Funktionsweise, Tarnung und Kompromittierung geschaffen. Ein Ziel haben sie jedoch gemein: Ihnen zu schaden.

Viele Verantwortliche unterschätzen insbesondere das Risiko von Malware. Betrifft mich das? Das wird doch nicht ausgerechnet mich treffen …

Die Realität zeigt, dass jeder betroffen sein kann, vom einfachen Bürger bis hin zu Herstellern von Sicherheitssoftware.

Seit Jahren nimmt die Verbreitung von Malware zu und täglich kommen neue Arten von Viren, Würmern und Trojanern hinzu. Zusätzlich variiert die Art und Weise der Infektionswege. Nach einer Studie von <kes> und Microsoft ist die „Infektion durch Schadsoftware" auf den ersten Platz der Gefährdungen für die Unternehmens-IT vorgerückt. 74 Prozent der Studienteilnehmer haben angegeben, dass sie in den letzten zwei Jahren von Schadsoftware-Vorfällen betroffen waren.

Methodik
Anhand von Beispielen mit einem fiktiven Opfer (Max Schmitt) werden im Workshop/Vortrag verschiedene Verbreitungswege, Funktionsweisen und

Auswirkungen von Schadsoftware erläutert und live demonstriert. Ergänzt werden diese Beispiele 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. Ebenso sind Anwender und Mitarbeiter eingeladen, die die technischen Zusammenhänge von Malware besser verstehen bzw. kennenlernen wollen.

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.