Live Hacking: Zielgerichtete Angriffstechniken auf IT-Infrastrukturen

(Möglicher) Vortragstitel
Max Schmitt – denn er weiß nicht, was er tut!
Max Schmitt als Sprungbrett einer Advanced Persistent Threat (APT)
Max Schmitt umgeben von komplexen, zielgerichteten und effektiven Angriffen auf seine Daten

Inhalt
Unternehmen hierzulande sind auf neue Formen von Angriffen auf ihre Firmennetze nur unzureichend vorbereitet. Unter Advanced Persistent Threat (APT), zu Deutsch „fortgeschrittene, andauernde Bedrohung", werden komplexe, zielgerichtete und effektive Angriffe auf kritische IT-Infrastrukturen und vertrauliche Unternehmensdaten verstanden. Bei solchen Angriffen geht es den Cyberkriminellen um wertvolle Unternehmens- und Mitarbeiterdaten wie etwa Businesspläne oder Patente für neue Produkte. Dabei konzentrieren sich die Angreifer auf die Ausnutzung von „Trusted Relationships", also Kontakten, denen ein Nutzer vertraut, und zwar über Soziale Netzwerke und/oder vertrauenswürdig aussehenden Spam.

Viele Verantwortliche unterschätzen das Risiko von APTs. 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. Im Zuge eines solchen Angriffes gehen Cyberkriminelle sehr zielgerichtet vor und nehmen gegebenenfalls großen Aufwand auf sich, um nach dem ersten Eindringen in ein System weiter in die lokale IT-Infrastruktur des Opfers vorzudringen. Das Ziel eines APTs ist es, möglichst lange unentdeckt zu bleiben. Typisch ist, dass die Täter sehr viel Zeit und Handarbeit investieren und Werkzeuge bevorzugen, die nur für einzelne, spezifische Aufgaben geeignet sind. User bzw. Mitarbeiter dienen hierbei häufig als Sprungbrett. Über infizierte Links und sehr fortschrittliche Schadsoftware verschafft sich der Angreifer einen Einstiegspunkt in die Organisation und kann sich ausbreiten, Daten und wertvolle Informationen sammeln.

Methodik
Anhand von Beispielen mit einem fiktiven Opfer (Max Schmitt) werden im Workshop/Vortrag verschiedene Angriffsszenarien erläutert und es wird live demonstriert, wie Cyberkriminelle heute vorgehen, um Angriffe auf die IT-Umgebung von Organisationen durchzuführen. Ergänzt werden diese Szenarien 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 APT 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.