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.

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.

Live Hacking: Praxisbeispiele für die Informations-gewinnung aus frei verfügbaren, offenen Quellen

(Möglicher) Vortragstitel
Max Schmitt – denn er weiß nicht, was er tut!
Max Schmitt im Fadenkreuz der Spione – Prism, NSA und Co. lassen grüßen

Inhalt
Die Enthüllungen von Edward Snowden nehmen kein Ende. Das Ausmaß der Spionageaffäre hat unsere schlimmsten Befürchtungen weit übertroffen. Industrie- und Wirtschaftsspionage sind längst kein Tabuthema mehr.

Aber was geben wir selbst über uns preis? Apps, Blogs, Chats, Web 2.0, Smartphones, Messenger und soziale Netzwerke eröffnen Nutzern neue Möglichkeiten, mit Freunden, Bekannten, Kollegen und der restlichen Welt in Kontakt zu bleiben und Informationen auszutauschen. Die Gefahren werden dabei aber schnell unterschätzt. Privatsphäre und Datenschutz sind längst nicht mehr die einzigen Themen, die in diesem Zusammenhang kontrovers diskutiert werden.

Auch Cyberkriminelle und Datenspione haben die Beliebtheit dieser Plattformen als Chance erkannt und nutzen die Gutgläubigkeit vieler Nutzer aus. Dabei werden Daten aus frei verfügbaren und offenen Quellen gesammelt, um durch Analyse der unterschiedlichen Informationen verwertbare Erkenntnisse zu gewinnen. In der Welt der Nachrichtendienste wird diese Methodik Open Source Intelligence (OSINT) genannt.

Methodik
Der Vortrag bietet einen Einblick in die Open Source Intelligence (OSINT) und in die Gefahren, die im Umgang mit digitalen Medien lauern. Anhand eines fiktiven Opfers (Max Schmitt) werden der Intelligence-Bedarf, effiziente Internet-Recherchen, Pflege des Quellenbewusstseins und Arbeit mit Offline-Informationsquellen erläutert und live demonstriert. Ergänzt werden diese durch Beispiele aus der Praxis.

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 Methoden von OSINT 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.

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.

Live Hacking: Praxisbeispiele für Angriffe auf kritische Infrastrukturen

(Mögliche) Titel
Live Hacking Industrial Control Systems (ICS) – Angriffsszenarien auf kritische Infrastrukturen
„Houston. Wir haben ein Problem!" - Angriffsszenarien auf kritische Infrastrukturen
Live Hacking Industrial Control Systems (ICS) – Angriff am Fließband
Die Entführung der U-Bahn Pelham 123 – ein Praxisbeispiel für Angriffe auf kritische Infrastrukturen
Gefahr in (Ver)Zug! – Praxisbeispiele für Angriffe auf kritische Infrastrukturen
Gefahr in (Ver)Zug! – Praxisbeispiele für Angriffe im Internet der Dinge (IoT – Internet of Things)
Live Hacking 4.0 – Sicherheitsrisiken von Industrie 4.0 und IoT verstehen
Live Hacking 4.0 – Industrie 4.0 und IoT: Im Land der unbegrenzten Möglichkeiten

Inhalt
Nach dem Megatrend Cloud Computing werden Industrie 4.0 und Internet der Dinge (IoT) abermals die bestehenden IT-Konzepte und -Prozesse in den Unternehmen verändern.

Durch das „Verheiraten" der Produktion mit der klassischen IT können Hacker-Angriffe drastische Folgen haben. Hackerangriffe und Cyber-Spionage auf kritische Infrastrukturen sind deshalb zu einer ständigen Bedrohung der industriellen IT geworden. Trojaner und Malware werden speziell dazu entwickelt, Produktions- und Versorgungsanlagen gezielt zu sabotieren oder Informationen über industrielle Steuerungsanlagen und Systeme zu sammeln. Dabei stehen Industriestaaten ganz besonders im Fokus.

„Aber kritische Infrastrukturen unterliegen doch strengen Sicherheitsvorgaben. Ein Angriff kann daher bestimmt nicht so einfach sein, oder?"

Leider doch! Neben hochkomplexen Cyberwaffen stellen insbesondere bekannte IT-Sicherheitslücken ein Risiko für Unternehmen und deren Produktionsanlagen dar. Die Vielfalt der Angriffsmöglichkeiten eröffnet eine neue Gefahrendimension. Der Verlust wichtiger Unternehmensdaten und schützenswerter Informationen ist schwerwiegend – wird jedoch gegenüber der Gefahr des Produktionsstillstands oder der Beeinflussung der Abläufe häufig als das „geringere Problem" betrachtet. Jeder erfolgreiche Angriff auf die industrielle IT bedeutet auch eine Bedrohung für Mensch und Umwelt!

Methodik

In Fallbeispielen wird konkret aufgezeigt, welche Methoden Cyberkriminelle verwenden, um Produktions- und Steuerungsprozesse 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 Inhalte eingegangen.

Zielgruppe
Der Vortrag richtet sich an Elektro-, Automatisierungs- und Prozessverfahrenstechniker bzw. Ingenieure, die sich mit dem Betrieb und der Administration von Automatisierungstechnik auseinandersetzen. Ebenso sind technische Entscheidungsträger und leitende Angestellte eingeladen, die die industrielle IT und deren Sicherheit besser verstehen bzw. kennenlernen wollen.

Voraussetzungen:	Basiskenntnisse (industrielle) IT, Automatisierungstechnik
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.

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.

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.

HackNight

(Möglicher) Eventtitel
HackNight – Der Kampf Gut gegen Böse
HackNight – Ein Blick auf die Anatomie von Cyberattacken

Inhalt
Hacker sind in den Medien allgegenwärtig – und werden gerne als Feindbild aus dem Hut gezaubert, um diffuse Bedrohungsszenarien zu illustrieren und Ängste zu schüren. Aber nur wenige von uns bekommen jemals die Gelegenheit, einem echten Hacker bei der Arbeit zuzusehen und sich selbst davon zu überzeugen, welche Gefahr von den Cyberkriminellen ausgeht und wie einfach manche Szenarien sind.

Im Rahmen der HackNight wird der Kampf „Gute gegen Böse" live demonstriert. Es wird aufgezeigt, mit welchen Tricks und Tools sich Hacker heute Zugang zu Netzwerken, Daten und Webanwendungen der Unternehmen verschaffen. Damit die Aufgabe des Hackers nicht zu einfach wird, stellt sich ihm ein Sicherheitsexperte als Verteidiger entgegen. Seine Aufgabe in diesem „Duell" ist es, die Attacken zuverlässig abzuwehren und Angriffen mit aktuellen Sicherheitslösungen wirksam einen Riegel vorzuschieben.

Besonders anschaulich ist dabei, dass sich die beiden Kontrahenten nichts schenken und immer wieder auf die Handlungen des jeweils anderen reagieren. Spannend ist insbesondere die Tatsache, dass sich beide im Vorfeld nicht absprechen, sondern lediglich ihr Ziel vor Augen haben. Zudem wird auf PowerPoint und sonstige Marketing-Schlachten verzichtet. Das Publikum kann sich live auf eine der beiden Seiten stellen und direkt auf die Geschehnisse einwirken. Der Spaßfaktor der Veranstaltung für das Publikum ist somit garantiert.

Hackazon 2.0
Hackazon 2.0 ist eine Web-Anwendung mit verschiedenen Schwachstellen (SQL-Injection, Cross-Site-Scripting, XML External Entity Attack usw.). Die Anwendung stellt einen Online-Shop zur Verfügung, der die gleichen Technologien verwendet wie modernen Web- und Mobile-Anwendungen. Hackazon 2.0 hat eine AJAX-Schnittstelle, Workflows und RESTful API. Zudem existiert eine Android Mobile App. Die Anwendung bietet für die Veranstaltung effektive Trainingsmöglichkeiten und eine Testplattform für Sicherheitsexperten. Dadurch können die zehn häufigsten Fehler laut „Open Web Application Security Project" (OWASP Top 10) in Web-Applikationen anschaulich analysiert und erläutert werden.

Methodik

Workshops über IT-Sicherheit müssen nicht immer „grau, trocken und unverständlich" sein. Die HackNight ist eine Mischung aus Präsentation, Übungen und Diskussion. Die Teilnehmer erhalten die Möglichkeit, für einige Stunden die Seiten zu wechseln, und erleben live, auf welche Art und Weise ihre Gegner vorgehen. Anhand diverser Beispiele werden verschiedene Angriffsszenarien erläutert und es wird live demonstriert, wie Cyberkriminelle heute vorgehen, um Angriffe auf Web-Anwendung und IT-Umgebung von Organisationen durchzuführen. Dem Auditorium werden die Inhalte anschaulich, unterhaltsam und vor allem nachhaltig vermittelt. Die Teilnehmer lernen, (Java-)Web-Anwendungen vor böswilligen Hacker-Angriffen zu sichern.

Zielgruppe
Die HackNight ermöglicht es, verschiedene Zielgruppen individuell anzusprechen, wie z. B. Anwender, Mitarbeiter, Führungskräfte, Administratoren, Software-Entwickler. Ebenso sind Personen eingeladen, die die Anatomie von Hackerangriffen besser verstehen bzw. kennenlernen wollen.

Voraussetzungen:	IT-Basiskenntnisse von Vorteil
Schwierigkeitsgrad:	leicht bis mittel

Eine zielgruppengerechte HackNight ist ebenfalls möglich.

Dauer
180 Minuten. Ein individueller und formatgerechter Zeitrahmen von 90 bis 300 Minuten ist ebenfalls möglich.

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.

Mythos Darknet – Verbrechen, Überwachung und Netzfreiheit in einem

(Möglicher) Vortragstitel
Darknet – Mythos und Realität: Reise in den digitalen Untergrund
Das Darknet – Eine Reise in die digitale Unterwelt
Das Darknet – Die dunkle Seite des Internets
Das Darknet – Was es ist und was es nicht ist
Darknet – Das „Dunkle Netz" verstehen und begehen

Inhalt
Google & Co. zeigen nur einen Teil des Internets. Was Suchmaschinen nicht automatisiert erfassen (können), bezeichnet man als Deep Web. Und dann gibt es da noch das Darknet, technisch gesehen ein komplett verschlüsselter Bereich des Internets.

Zuletzt ist das Darknet durch den Amokläufer von München in die politische Diskussion geraten, weil er seine Waffe in diesem Teil des Internets besorgt hat.

Dieses „Paralleluniversum" dient nicht nur illegalen Zwecken, wie gemeinhin angenommen wird. Dennoch hat das Darknet massiv an Bedeutung in der Hacker-Community gewonnen, die es als Handelsplattform für illegale Geschäfte nutzt. Die Zahlen sprechen für sich. Die Internetkriminalität breitet sich aus. Die polizeilichen Statistiken bilden jedoch nur einen Ausschnitt der tatsächlichen Dimension des Cybercrimes ab. Hinzu kommt eine Dunkelziffer von unentdeckten Fällen. Im Darknet werden Angriffe vorbereitet, Beute wird zum Verkauf angeboten. Das BKA zog alleine in den letzten vier Monaten fünf Marktplätze aus dem Verkehr. Die Täter gehen dabei dezentral vor, oft einzeln, aber auch in Gruppen, die sich wieder trennen. Auch längerfristige Zusammenschlüsse in der Art organisierter Kriminalität nehmen zu. Dadurch wird Internetkriminalität zu einer zunehmenden Bedrohung für Unternehmen.

Nur wer sich auskennt, hat die Chance, sich in dieser virtuellen Welt zu bewegen, zu recherchieren und sich entsprechend zu wappnen, und kann sich vor allem sein eigenes Bild machen. Dazu sind grundlegende Kenntnisse der Werkzeuge und Methoden notwendig.

Ziel des Vortrags ist es, diese Kenntnisse zu vermitteln, um damit über die Funktionsweise des Darknets aufzuklären und einen Einblick in diesen Teil des Internets zu verschaffen.

Methodik
Im Vortrag werden die Teilnehmer in die Welt des Darknets eingeführt, die für die meisten Anwender unbekannt ist. Es wird gezeigt, wie sich Kriminelle im verschlüsselten Teil des Internets bewegen, welche Möglichkeiten und Inhalte sich dort bieten und welche Gefahr davon für Unternehmen ausgeht.

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

Zielgruppe
Der Vortrag richtet sich insbesondere an die IT-Verantwortlichen im Unternehmen oder in der Organisation, aber auch an Manager, Führungskräfte und Abteilungen anderer Fachrichtungen, die die Funktionsweise und die Gefahren des Darknets besser verstehen wollen.

Voraussetzungen:	IT-Basiskenntnisse von Vorteil
Schwierigkeitsgrad:	leicht bis mittel

Eine zielgruppengerechte Präsentation und ein Keynote Speech sind 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 neueste (Forschungs-)Erkenntnisse der Branche.

Vita (mittel)

Marco Di Filippo ist 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 neueste (Forschungs-)Erkenntnisse der Branche.

Vita (kurz)

Marco Di Filippo ist Autor, Blogger, Berater und hält Fach- und Publikumsvorträge. Sein Spezialgebiet sind organisatorische und technische IT-Sicherheitsprüfungen und -konzepte.