

Kapsch Security Day 2016

22. Juni 2016, Tagungszentrum Schönbrunn

Das Programm

Uhrzeit			
08.30	Check-in & Breakfast		
09.15 – 09.25	Begrüßung durch Dr. Franz Semmernegg CEO Kapsch BusinessCom		
09.25 – 09.50	Digitalisierung und Malware – ein rasanter Anstieg Robert Jankovics & Franz Stögerer Kapsch BusinessCom	Tech.	
09.50 – 10.35	Kapsch Managed Defense. Monitor.Detect.Respond. Timo Jobst & Thomas Mann Kapsch BusinessCom	Tech.	
10.35 – 11.00	Coffee Break in der Partner Area		
	Track 1	Track 2	Track 3
11.00 – 11.20	Microsoft Cybercrime Center Harald Leitenmüller Microsoft Österreich	Tech.	Umfassender Schutz von Symantec Martin Werner Symantec
11.25 – 11.45	One step ahead – Version R80, eine ganzheitliche Security-Lösung Roman Prinz Check Point Österreich	Tech.	Industrie 4.0 – Paradies für Cyberkriminalität? Stefan Podhajski Kapsch BusinessCom
11.50 – 12.10	Securing Industry 4.0 Klaus Gheri Barracuda Networks	Tech.	New Workspace – tägliche Security-Herausforderungen für das Unternehmen Martin Weilhartner Citrix Systems
12.15 – 12.35	Ransomware kennt keine Grenzen – das muss nicht sein! Rene Fleissner-Lichtel Palo Alto Networks	Tech.	Sie können nur absichern, was Sie sehen! Eduard Serkowitsch ForeScout Technologies
12.35 – 13.40	Lunch Break in der Partner Area		
13.40 – 14.10	It takes a network to defeat a network Philipp Amann Leitung Strategy & Development Europol – European Cybercrime Centre (EC3)		
14.10 – 14.40	Aufgaben und Befugnisse der Aufsichtsbehörde nach der Datenschutz-Grundverordnung Matthias Schmid Österreichische Datenschutzbehörde		
14.40 – 15.10	Coffee Break in der Partner Area		
	Track 1	Track 2	Track 3
15.10 – 15.30	Die Abdeckung des gesamten Angriffscontinuums Britta Paty Cisco Systems	Tech.	Optimale Absicherung von Cloud-Applikationen Eduard Decker Blue Coat Systems
15.35 – 15.55	Ist ausreichende Security heute ausreichend? Andreas Senn FireEye Österreich	Tech.	Die Balance zwischen Technik und Organisation im Bereich der Informationssicherheit Thomas Mann Kapsch-Gruppe
16.00 – 16.20	Die Zeit ist reif für eine vereinfachte Bedrohungsabwehr – Schützen. Erkennen. Korrigieren. Paul Zotlöterer & Andreas Schober Intel Security Austria	Tech.	Sichere Authentifizierung – unkompliziert, jederzeit und überall Dirk Losse HID
16.25 – 17.15	Sind Sie reif für eine Digital-Therapie? Ein Impulsvortrag von Digital-Therapeutin und Bestseller-Autorin Anitra Egger		
17.15 – 17.30	Finale mit Verlosung einer Apple Watch unter allen Teilnehmern		
ab 17.30	Barbecue und EM-Live-Übertragung Österreich gegen Island auf XL-LED-Wall		

Kapsch Security Day 2016

22. Juni 2016, Tagungszentrum Schönbrunn

Das Programm im Detail

Uhrzeit			
08.30	Check-in & Breakfast		
09.15 – 09.25	Begrüßung durch Dr. Franz Semmernegg CEO Kapsch BusinessCom		
09.25 – 09.50	Digitalisierung und Malware – ein rasanter Anstieg Tech. Je mehr die Digitalisierung um sich greift, umso mehr Ausbreitungsmöglichkeiten gibt es für Malware. Sicherheitsbedrohungen und -lösungen rücken noch stärker in den Fokus unseres Geschäftslebens und benötigen die entsprechende Aufmerksamkeit. Effizientes Business braucht wirksame Security – erfahren Sie gleich zu Beginn des Security Days, wie diese aussehen kann. <i>Robert Jankovics & Franz Stögerer</i> Kapsch BusinessCom		
09.50 – 10.35	Kapsch Managed Defense. Monitor.Detect.Respond. Tech. Präventive Schutzmaßnahmen, die in den meisten Unternehmen heutzutage eingesetzt werden, können einige bösartige Aktivitäten blockieren. Trotzdem wird es immer schwieriger, die eigene Organisation zu schützen, da die Angreifer immer raffiniertere Taktiken anwenden. Aus diesem Grund müssen wir den Blickwinkel auf Angriffe ändern. Es geht heute nicht mehr nur darum, den Angriff selbst zu verhindern, sondern das Erreichen der klar definierten Ziele der Angreifer zu vereiteln. Die entsprechende Visibility im Unternehmen und die richtigen Analysetechniken ermöglichen es, Eindringlinge zu erkennen, richtig zu reagieren und den Angriff einzudämmen. Am Beispiel der Kapsch Gruppe wird demonstriert, wie die Balance zwischen Technik und Organisation im Bereich der Informationssicherheit gefunden wird, um dadurch eine Lösung wie das Kapsch Managed Defense Service argumentieren und realisieren zu können. <i>Timo Jobst, Cyber Security Analyst & Thomas Mann, CISO</i> Kapsch BusinessCom		
10.35 – 11.00	Coffee Break in der Partner Area		
	Track 1	Track 2	Track 3
11.00 – 11.20	Microsoft Cybercrime Center Tech. Microsoft hat vor einiger Zeit das Cybercrime Center eröffnet. Hier gehen Anwälte und Sicherheitsexperten der Schwergewichte der IT-Branche mithilfe neuester Technologien und ihrem Expertenwissen gegen Online-Kriminalität vor. Die primären Ziele des Cybercrime Centers sind die Bekämpfung von IP-Kriminalität, Schadsoftware – hier vor allem von Botnets – sowie die Bekämpfung der Ausbeutung von Kindern. Hierzu wird eng mit Ermittlungsbehörden, Hochschulen, der Industrie und NGOs zusammengearbeitet. Diese Einrichtung wird auch unter den Insidern „CSI: Hackers“ bezeichnet. <i>Harald Leitenmüller</i> CTO, Microsoft Österreich	Umfassender Schutz von Symantec Tech. Von Ransomware bis hin zu ausgeklügelten APTs: Die IT-Bedrohungslage steigt stetig an. Symantec zeigt intelligente und proaktive Schutzmaßnahmen, die Ihre Daten schützen und Ihr Unternehmen auch für zukünftige Security-Herausforderungen rüstet. <i>Martin Werner</i> Presales Consultant, Symantec	Industrie 4.0 – Paradies für Cyberkriminalität? Die fortschreitende Vernetzung von Maschinen, Produkten und Menschen in der Industrie bringt neben signifikanten Vorteilen auch große Herausforderungen im Security-Umfeld mit sich. Der Einsatz von entsprechenden Technologien verringert zwar das Risiko von Cyberkriminalität signifikant, reicht aber nicht aus, um sich bestmöglich davor zu schützen. Der jährliche weltweite Schaden beläuft sich auf 400 Milliarden USD, Tendenz steigend. <i>Stefan Podhajski</i> Business Development Manager, Kapsch BusinessCom
11.25 – 11.45	One step ahead – Version R80, eine ganzheitliche Security-Lösung Tech. Die stark zunehmende Anzahl an Sicherheitsvorfällen zeigt auch österreichischen Betrieben die Vorteile und Notwendigkeit einer ganzheitlichen Security-Lösung auf. Besorgniserregend ist die Zunahme von Attacken mit unbekanntem Signaturen, daher ist ein Strategiewechsel in der IT-Sicherheit notwendig – weg von der Erkennung zur Verhinderung von Cyberangriffen. Neben der technischen Marktführerschaft bei Next-Generation Firewall-Funktionen und dem Schutz vor noch unbekanntem Bedrohungen nehmen organisatorische Maßnahmen zunehmend eine wichtige Rolle in der Umsetzung ein. Kunden aller Größenordnungen sollen bei der Entwicklung von Strategien unterstützt werden – Ziel ist es, der wachsenden Gefahr durch cyberkriminelle Malware weiterhin „one step ahead“ zu sein. <i>Roman Prinz</i> Country Manager, Check Point Österreich	New Workspace – tägliche Security-Herausforderungen für das Unternehmen Tech. Definition des neuen flexiblen Arbeitsplatzes und welche Herausforderungen dieser für den täglichen Betrieb im Unternehmen mit sich bringt. Design und Architektur speziell hinsichtlich Security und Citrix-Lösungsansätze für die Umsetzung. <i>Martin Weilharter</i> System Engineer, Citrix Systems	Sie können nur absichern, was Sie sehen! Die Frage „Welche Geräte genau sind gerade jetzt in unserem Netzwerk und sind sie sicher?“ treibt heute vielen IT- und Sicherheitsverantwortlichen den Schweiß auf die Stirn. Zunehmende Angriffshäufigkeit, Komplexität, Mobilität und das heranrückende Internet of Things machen es notwendig, Geräte in der Sekunde, in der sie sich mit dem Netzwerk verbinden, zu erkennen, zu klassifizieren, zu überwachen und vor allem ihren Zugriff zu regeln. <i>Eduard Serkowsch</i> Senior Systems Engineer, ForeScout Technologies
11.50 – 12.10	Securing Industry 4.0 Das Internet der Dinge (IoT) und Industrie 4.0 werden immer wichtiger. Viele Unternehmen jeder Größenordnung stehen nun vor neuen Herausforderungen – wie sichere ich Tausende von Remote-Geräten ab und wie manage ich diese effizient? Die NextGen-Firewall S-Serie von Barracuda wurde genau dafür entwickelt. <i>Klaus Gheri</i> Barracuda Networks	Optimale Absicherung von Cloud-Applikationen Tech. > Shadow-IT – welche Cloud-Applikationen nutzen Sie und welche werden „unsichtbar“ von Mitarbeitern im Firmennetz genutzt? > Kontrolle der Cloud-Applikationen – wer darf Dokumente in die Cloud stellen und wer darf sie lesen? > SaaS-Cloud Anbieter (Salesforce, ServiceNow ...) – warum Inhalte und Anwendungen verschlüsseln? > Ist es wichtig „in the cloud“ Sichtbarkeit von Applikationen und Daten, Zugangskontrolle in die Cloud und Datenschutz zu haben? <i>Eduard Decker</i> Senior Systems Engineer, Blue Coat Systems	Die Balance zwischen Technik und Organisation im Bereich der Informationssicherheit Org. > Das Umfeld wird immer dynamischer und globaler (sowohl unternehmensintern als auch im Bereich der Bedrohungen) > Die richtige Organisation und präventive Maßnahmen (Audit, Governance) bilden die Basis > Professionelles Information Security Incident Handling im Rahmen des Kapsch SIRT > Sicherheitsbedrohungen monitoren, erkennen und entsprechend reagieren > Erweiterte Sicherheitstechnologien im Bereich APT sowie professionelle internationale Unterstützung sichern den Erfolg <i>Thomas Mann</i> Chief Information Security Officer, Kapsch-Gruppe
12.15 – 12.35	Ransomware kennt keine Grenzen – das muss nicht sein! Tech. Ransomware und Daten haben per se keine Grenzen, herkömmliche Sicherheitslösungen sehr wohl. Damit Ihre Business-Daten umfassend und wirksam vom Endpoint bis in die Cloud geschützt sind, braucht es neue Lösungen. Palo Alto Networks sorgt dafür, dass die Kontrolle Ihrer Daten bei Ihnen bleibt. Erleben Sie, wie das möglich ist. <i>Rene Fleissner-Lichtel</i> System Enginner, Palo Alto Networks	Sichere Authentifizierung – unkompliziert, jederzeit und überall Tech. HID Global ermöglicht mit der Plattform ActivID Tap Authentication die komfortable und zugleich sichere Multifaktor-Authentifizierung bei der Anmeldung zu Cloud-Anwendungen und webbasierten Diensten. Anwender halten dafür einfach ihre Smartcard an das jeweilige Notebook, Tablet, Smartphone oder an andere NFC-kompatible Geräte und kommen somit ohne komplexe Passwörter aus. Dafür verwenden sie die bereits für die Zutrittskontrolle vorhandenen Seos-Credentials auf einer Karte. <i>Dirk Losse</i> Presales Manager IAM Solutions, DACH HID	EinBlick in die Cloud aus rechtlicher Sicht Org. > Safe Harbor, Facebook und die Folgen > Aktuelle Entwicklungen > Allgemeine rechtliche Überlegungen <i>Christian Urban</i> Leitung Recht, Kapsch BusinessCom
12.35 – 13.40	Lunch Break in der Partner Area		
13.40 – 14.10	It takes a network to defeat a network > Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und die Industrie als wichtige Partner > Einblick in Aufbau, Aufgabenbereich und Tätigkeit des EC3 > Überblick über die Entwicklungen im Bereich Cyberkriminalität > Mit welchen Herausforderungen ist zu rechnen? > Ideen zu den Gegenmaßnahmen, die wir treffen können <i>Philipp Amann</i> Leitung Strategy & Development Europol – European Cybercrime Centre (EC3)		
14.10 – 14.40	Aufgaben und Befugnisse der Aufsichtsbehörde nach der Datenschutz-Grundverordnung > Welche Aufgaben hat die Aufsichtsbehörde? > Welche Befugnisse hat die Aufsichtsbehörde zur Durchsetzung von Rechtsvorschriften (Bescheide, Geldbußen)? > In welchen Angelegenheiten komme ich mit der Aufsichtsbehörde in Kontakt? > In welchen Fällen kann sich die Aufsichtsbehörde an Unternehmen wenden? <i>Matthias Schmidl</i> Stv. Leiter der Österreichischen Datenschutzbehörde		
14.40 – 15.10	Coffee Break in der Partner Area		
	Track 1	Track 2	Track 3
15.10 – 15.30	Die Abdeckung des gesamten Angriffskontinuums Tech. Cisco verfügt über das branchenweit umfangreichste Portfolio an Systemen für eine fortschrittliche Bedrohungsabwehr. Durch seinen bedrohungsorientierten Ansatz mit leistungsstarker Korrelation sowie kontinuierlicher und kontextbasierter Malwareanalyse verringert Cisco die Komplexität. Cisco's Ecosystem Collective Security Intelligence (CSI) ermittelt Entwicklungen in der Bedrohungslandschaft anhand von Telemetriedaten aus Sensoren und Active Threat Analytics und sorgt für eine effektive Absicherung, eine schnelle Erkennung und eine zügige Reaktion. <i>Britta Paty</i> Security Solution Specialist, Cisco Systems	SSL everywhere Tech. Nicht nur die bekannten SSL-Schwächen wie POODLE und Heartbleed, auch die Diskussionen rund um Abhörsicherheit und das legitimierte wie auch das nicht legitimierte Mitlesen privater Nachrichten rücken das Thema SSL wieder verstärkt in den Vordergrund. Doch wie erreicht man perfekte Sicherheit mit der „Verschlüsselung der einfachen Leute“? Und wie geht man im Sinne von Security Management richtig damit um, wenn nun alles verschlüsselt ist? Wie und wo wird aufgebrochen oder doch lieber terminiert? Und wie lässt sich ein Air Gap füllen? <i>Roman Borovits</i> System Engineer F5 Networks	Künstliche Videointelligenz Phys. Nachhaltige Personenanalyse, Prozessüberwachung und Automatisierung durch den Einsatz von künstlicher Videointelligenz. Welche branchenunabhängigen Chancen und Möglichkeiten bieten sich dadurch für Unternehmen? <i>Wolfgang Baumgartner</i> Geschäftsführer, NETAVIS Software
15.35 – 15.55	Ist ausreichende Security heute ausreichend? Tech. Wie konnten Cyberkriminelle 2015 die angeblich unüberwindbaren Schutzmaßnahmen so vieler multinationaler Konzerne mit riesigen IT-Budgets knacken? Erfahren Sie, wie Sie sich auf Cyberangriffe vorbereiten und diese effizient abwehren können. Welche Branchen aktuell am stärksten gefährdet sind und worauf Sie beim Schutz vor gezielten Cyberangriffen im Speziellen achten sollen. Und was die NIS-Direktive der EU für Sie bedeutet. <i>Andreas Senn</i> Country Manager, FireEye Österreich	Nostalgie-Slot: Viren- und Malware-Zeitreise „de luxe“ Tech. Können Sie sich noch an Pong, C64 und High Memory erinnern? Kommen Sie mit auf eine IT-Security-Zeitreise in die Vergangenheit: Wir drehen die Zeit gemeinsam um 30 Jahre zurück und erleben noch einmal live die Entwicklung der Viren- bzw. Malwarelandschaft. <i>Hannes Trunde & Christian Kurta</i> Security Solutions Team, Kapsch BusinessCom	Interaktive Leitstandtechnologie Phys. Effizienzsteigerung bei Human-Machine Interfaces (HMI) durch einfache, intuitive und anwenderunterstützte GUIs. Mehrwerte durch interagierende Leitstandtechnologie sowie Prozessoptimierung durch vordefinierte und automatisierte Szenarien. <i>Christoph Reichl</i> Geschäftsführer, RC-TEC
16.00 – 16.20	Die Zeit ist reif für eine vereinfachte Bedrohungsabwehr: schützen. Erkennen. Korrigieren. Tech. Mit seiner Security-integrated-Strategie, einem innovativen Ansatz für hardwareunterstützte Sicherheitslösungen und einem Global-Threat-Intelligence-Netzwerk fokussiert sich Intel Security auf die Bereitstellung von proaktiven, bewährten Sicherheitslösungen, die Systeme weltweit schützen. Zielsetzung von Intel Security ist es, sicheres Agieren und Arbeiten in der digitalen Welt zu gewährleisten. <i>Paul Zotlöterer & Andreas Schober</i> Intel Security Austria	Live-Demo: Ein Klick reicht aus! Tech. Perfekt auf unsere De-luxe-Zeitreise abgestimmt, gehen wir natürlich auch auf aktuelle IT-Bedrohungsszenarien ein. Neben einer Live-Demo zum Thema CryptoLocker möchten wir vor allem aufzeigen, dass nur das Zusammenspiel aller Abteilungen und Bereiche in einem Unternehmen diese modernen Angriffe verhindern kann. <i>Florian Bogner & Christian Kurta</i> Security Solutions Team, Kapsch BusinessCom	Physical Security Consulting Phys. Wie kann sich ein Unternehmen den aktuellen Bedrohungen in den Bereichen Industrie- und Wirtschaftsspionage stellen, den Schutz des geistigen und physikalischen Eigentums gewährleisten und ein zeitgemäßes Konzept für einen nachhaltigen und sicheren Betrieb erlangen? <i>Alex Andrzejewski</i> Sales Expert, Kapsch BusinessCom
16.25 – 17.15	Sind Sie reif für eine Digital-Therapie? E-Mail, Handy, Web, Social Media: Wir sind dauerabgelenkt, statt aufmerksam. Sie reagieren, statt zu agieren. Wir sind überkommuniziert, aber uninformiert. Kennen Sie die 69. Website hinten links, auf der Sie sich fragen, was Sie vor einer Stunde eigentlich gemacht haben, als Sie „nur mal kurz was googeln“ wollten? Dann wird's Zeit für eine Digital-Therapie! Rezeptfrei, radikal, wirkungsvoll. Nach diesem Blitz-Therapie-Vortrag wissen Sie, wie Sie die Macht über Ihre Kommunikation zurückgewinnen, stressfrei erfolgreich kommunizieren und Ihrem „Internet-Ich“ eine 1a-Reputation verleihen. Ein Impulsvortrag von Digital-Therapeutin und Bestseller-Autorin <i>Anitra Eggl</i>		
17.15 – 17.30	Unter allen Teilnehmern		
ab 17.30	Barbecue und EM-Live-Übertragung Österreich gegen Island auf XL-LED-Wall		