IT-Strategie und Security Konferenz

Veranstaltung: »IT-Strategien umsetzen, Technologietrends bewerten und Innovationsmanagement« und »Security Trends – Cybersecurity – Artificial Intelligence – Sichere Architekturen« wurde am 15. 11. 2022 von Future Network und CON•ECT Informunities im Palais Eschenbach in Wien (hybrid) veranstaltet (www.conect.at).

In einer zunehmend vernetzten und technologiegetriebenen Geschäftswelt ist das Thema Vertrauen wichtiger denn je. Fast jedem zweiten Unternehmen weltweit gelingt es jedoch nicht, sich adäquat gegen digitale Bedrohungen zu wappnen und sie riskieren dadurch den Verlust des Vertrauens ihrer Kunden und der Gesellschaft: Nur gut die Hälfte der Unternehmen (53 Prozent) integriert Maßnahmen zum Management von Cyber und Datenschutzrisiken vollständig von Beginn an in ihre digitalen Transformationsprojekte. Zu diesem Ergebnis kommen die Digital Trust Insights, eine internationale Befragung von 3000 Führungskräften in 81 Ländern im Auftrag von PwC.

So zeigte die Studie etwa, dass Sicherheitsvorkehrungen vielfach nicht mit den Geschäftszielen in Einklang gebracht werden, Sicherheitsmaßnahmen aufgrund fehlender Hintergrundinformationen zu potenziellen Angreifern kaum risikoorientiert eingesetzt werden oder Security- und Privacy-Experten oftmals viel zu wenig in Digitalisierungsprojekten eingebunden werden.

(Quelle: Digital Trust Insights 2019 von Price Waterhouse)

Keynotes der Veranstaltung Security-Trends

Cyber Security by Design: Angriffspfade in der Systemarchitektur erkennen, bevor es zu spät ist

Christoph Schmittner (AIT)

Wie kann man Angriffspfade in der Systemarchitektur erkennen, bevor es zu spät ist? Christoph Schmittner (AIT) sprach live bei der Security-Veranstaltung über Cyber Security by Design als Gamechanger, welcher System-Anforderungen reflektiert, so wie wir sie heute im sicherheitskritischen IoT Umfeld antreffen.

Es wurde gezeigt, wie das Security Operation Center, das SOC, als »Blue Team« durch ein internes »Red Team« gleichsam in einem Katz- und Maus-Spiel immer wieder herausgefordert und getestet wird. Diese Vorgehensweise hilft dabei, existierende Schwachstellen und Lücken zu identifizieren und zu bearbeiten. Dargestellt wurde das anhand eines Beispiels einer Zero-Day Schwachstelle.

Über den internen Zuwachs von Wissen und Erfahrungen ist auch die Kommunikation in »Trusted Communities«, wie dem Austrian Energy CERT ein wichtiger Faktor in der Bewältigung der aktuellen Herausforderungen, sowie die Einbindung von internationalen Threat Feeds um immer auf den neusten Stand zu sein.

In den vergangenen drei Jahren haben wir eine umfangreiche Systemlandschaft aufgebaut, welche wir gerne vorstellten und auch unseren Ansatz eines effizienten und effektiven Security Teams.

Vortragender: Christoph Schmittner (Austrian Institute of Technology, wissenschaftlicher Mitarbeiter im Bereich Safety and Security)

Ransomware: sicher verschlüsselt! – Festplatte: verschlüsselt sicher?

Michael Strametz (SySS)

Die Daten wurden »sicher« verschlüsselt durch Ransomware! Warum funktioniert das »Geschäftsmodell« Ransomware so gut? Warum Lösegeld auch schon »gewinnbringend« veranlagt wurde und warum Kapital trotzdem besser nicht in Form von Lösegeldzahlungen veranlagt werden sollte.

Im Gegensatz dazu stehen externe Speichermedien wie Festplatten oder USB-Sticks, die extra damit werben sicher zu sein, weil eine AES-Hardwareverschlüsselung implementiert ist. Bei diesen Geräten ist es oftmals möglich die gespeicherten Daten zu entschlüsseln. SySS zeigte die aktuellen Ergebnisse einer Forschungsarbeit anhand eines praktischen Beispiels.

Vortragender: Michael Strametz (SySS Cyber Security GmbH, Standortleiter Österreich, IT-Sicherheitsexperte)

Cyber Defense in einem Unternehmen der kritischen Infrastruktur

Für Betreiber kritischer Infrastrukturen sind die Security-Anforderungen nicht nur durch die generell steigende Bedrohungslage höher geworden, sondern auch durch gesetzliche Anforderungen und die steigende Digitalisierung.

Aus unserer Sicht lassen sich alle Aufgaben der IT/OT-Security und Informationssicherheit in drei Bereiche zusammenfassen. Diese sind in strategische, offensive und defensive Bereiche gegliedert. Eine Zusammenarbeit dieser Bereiche ist unabdingbar, da sie voneinander abhängig sind und voneinander bzw. miteinander lernen können.

Im defensiven Bereich setzt man hierfür zum Beispiel ein Security Operations Center (SOC) ein. Es hat die Aufgabe, alle IT/OT-Systeme zu überwachen unabhängig von Hard- oder Software, und gegebenenfalls mit Unterstützung von international agierenden Partnern (z. B. AEC). Das SOC ist außerdem in enger Abstimmung mit den anderen beiden Bereichen (strategisch und offensiv).

Eine Kernfrage, die sich uns beim Aufbau des SOC gestellt hat war, wie neue Angriffsmethoden erkannt werden können und man diese testen kann. Gerade bei neuen Zero-Day Schwachstellen ist es wichtig zu überprüfen ob die eigenen Systeme verwundbar sind und das SOC eine Ausnutzung dieser erkennt.

Um diese Frage beantworten zu können, bedarf es interner White-Hat-Hacker, welche anhand von neuen Angriffstechniken versuchen, in Systeme einzudringen. Sie versuchen öffentlich verfügbare PoCs (Proofs of Concept) auf das Unternehmen und dessen Infrastruktur anzupassen oder eigene zu entwickeln, um Schwachstellen auszunutzen und einer Erkennung durch das SOC zu entgehen.

Durch dieses Vorgehen entsteht eine kontinuierliches Katz-und-Maus-Spiel. Ein solches lässt sich auch bei Anti-Viren Programme beobachten. Erste Anti-viren Programme arbeiteten signatur-basiert. Da Angreifer jedoch diese Signaturen umgehen konnten, zum Beispiel durch den 1-Byte Change Trick wo das erste Byte von Shellcode verändert wird, mussten neue Erkennungsmethoden entwickelt werden. Erste Anti-Viren- / EDR-Software begann über sogenannte Syscall Hooks die Funktionsaufrufe der WinAPI zu überwachen. Da diese Hooks im User Space definiert wurden, war es Angreifern möglich diese bei Programmstart zu entfernen, zum Beispiel indem die WinAPI-Module neu in den Speicher geladen werden. Da diese Methode aktuell nicht mehr ausreicht um maliziöses Verhalten zu erkennen, verwenden aktuelle EDRs eine Kombination aus unterschiedlichen Quellen (z. B. Hooks im User-Land / Kernel-Land, dem Microsoft Etw-Ti Provider) um Funktionsaufrufe überwachen zu können.

Ein Beispiel aus der Praxis ist die Schwachstelle Follina. Hier wurde durch das Red Team ein eigener Proof of Concept entwickelt und getestet, ob der Code auf den Clients des Unternehemens ausgeführt werden kann. Gleichzeigt hat das Red Team Feedback vom Blue-Team bekommen, ob diese Angriffe erkannt wurden. Da zu diesem Zeitpunkt weder das EDR-Tool, noch die NTA (Network Traffic Analysis), und auch nicht die E-Mail-Security-Lösung den Angriff erkannt haben, hat das Red-Team gemeinsam mit dem Blue-Team Indicators of Compromise definiert und daraus eine Hunting Query erstellt. Diese wird regelmäßig ausgeführt und benachrichtigt das Blue-Team, wenn ein neuer Angriffsversuch erkannt wird. Gleichzeitig entwickelt das Blue-Team Gegenmaßnahmen um die Schwachstelle auf den eigenen Systemen zu schließen.

Durch das ständige Testen von neuen Angriffen und der Erkennung dieser kann behauptet werden, dass ein einzelnes IT/OT-Security System zur Erkennung von Angriffen bei weitem nicht ausreicht. Daraus ergibt sich eine Systemlandschaft aus verschiedenen Tools sowohl für das Red-Team als auch für das Blue-Team.

Wichtig hierbei sind nicht die Produkte im Detail sondern die Kombination und Verschneidung der Fähigkeiten dieser Produkte. Wichtig für uns war eine einheitliche Sicht auf alle Security Alerts im Unternehmen. Deswegen war unser primärer Ansatz, alle Informationen in einem Ticket-Tool zu sammeln, um diese gesammelt darstellen zu können.

Die einzelnen Security Tools bilden eine Art Puzzle für das SOC und erkennen unterschiedliche Angriffsvektoren vom OSI Schichtenmodell 2–7.

Vortragende: Florian-Sebastian Prack, MSc. ist Absolvent der FH St. Pölten. Er hat bei VERBUND als Projektleiter das SOC aufgebaut und hat sich darüber hinaus auf OT-Security spezialisiert. Seine Masterarbeit an der FH Technikum Wien behandelte das Thema »Vorgehensweise zur Implementierung eines Small Hybrid Security Operation Center«.

Paul Mader, MSc. ist im Security Engineering Team von VERBUND tätig und führt unter anderem Penetration Tests durch. Er schloss sein Masterstudium in IT-Security an einer englischen Universität ab. Aktuell beschäftigt er sich verstärkt mit den Themen Exploit Development und EDR-Evasion.

Keynotes der Veranstaltung IT-Strategien umsetzen

Leitfaden zum Erstellen und Umsetzen einer erfolgreichen IT-Integrationsstrategie – Rahmenwerk, Roadmapping, Implementation, Governance

Ernst Tiemeyer (IT-Consultant)

Der Wunsch nach einer umfassenden und nachhaltigen Integration der Business-IT-Landschaft stellt für viele Organisationen nach wie vor eine echte Herausforderung dar, bietet gleichzeitig aber auch gigantische Potenziale. Im Rahmen seines Vortrags stellte Ernst Tiemeyer ein in der Praxis bewährtes Vorgehensmodell zum Erstellen und Umsetzen einer erfolgreichen Integrationsstrategie vor.

Cloud-Technologien mit modernisierter Anwendungsintegration, IoT, Daten-Virtualisierung sowie B2B-Lieferketten haben zur Konsequenz, dass mittels einer hybriden Integrationsplattform sowohl auf der Entwicklungs – als auch auf der Managementebene neue Möglichkeiten für die IT-Integration genutzt werden müssen. Dies betrifft sowohl die Integration von Applikationen und Daten, aber

auch neue Formen wie Prozess-, Partner- sowie Infrastruktur- und Netzwerkintegrationen.

Enterprise IT-Verantwortliche stehen vor der Herausforderung, im Team eine nachhaltige Integrationsstrategie zu entwickeln und umzusetzen. Insbesondere das Vorliegen einer Business-Strategie sowie von Digitalisierungs-, Cloud-, Daten-, und Servicestrategien bilden dafür eine gute Basis.

Ein Rahmenkonzept, Handlungsfelder und Roadmaps für eine Integrationsstrategie werden in dem Beitrag ebenso aufgezeigt wie die Implementation bzw. die Governance der Integrationslösungen.

Vortragender: Ernst Tiemeyer (IT-Consultant, Projektmanager und Consultant für strategisches IT-Management und EAM – GfB)

IT Managed Services smart, sicher und individuell aufbauen – Ein Erfahrungsbericht der Modis IT Outsourcing GmbH aus dem komplexen Umfeld einer öffentlichen Verwaltung

Claudia Borst & Sven Lehmann (Akkodis)

Interessieren Sie sich dafür, wie IT Managed Services smart, sicher und individuell aufgebaut werden können? Claudia Borst und Sven Lehmann von Akkodis (früher Modis Deutschland) sprachen darüber und zeigten einen Erfahrungsbericht aus dem komplexen Umfeld einer öffentlichen Verwaltung!

An einem Kundenbeispiel mit umfangreichem IT-Bedarf, beleuchteten wir die im Projekt gemeinsam mit dem Kunden gesammelten Erfahrungen.

Wir reflektierten die komplette Prozesskette, von der Anschaffung der Hard-und Software, über Betrieb und Monitoring von Server und Netzwerk sowie Service Desk, Onsite Support und das Aufsetzen von IT-Prozessen.

Die Transition und der Betrieb aus den Perspektiven eines Kunden und eines Dienstleisters für Managed Services stehen im Fokus.

Schwerpunkte des Vortrages lagen auf dem Mehrwert für das Business in diesem Serviceumfeld, die erkannten »lessons learned« und die »best practices«.

Da Sicherheitsanforderungen und Datenschutz mehr denn je wichtig Themen sind, teilten wir auch hierzu neue Informationen und Erfahrungen.

Benchmarking: Wie gut ist Ihr IT-Service-Management? Wenn man es nicht messen kann, kann man sich nicht verbessern

Jens Leucke (Freshworks)

IT-Service-Management erfordert die Messung, Bewertung und Verbesserung von IT-Service-Prozessen. Metriken und KPIs liefern quantifizierbare Informationen über den Status Ihres Services, zeigen Möglichkeiten zur Serviceverbesserung auf und geben Aufschluss über den Fortschritt bei der Erreichung Ihrer Geschäftsziele. Sie möchten die wichtigsten Leistungskennzahlen entdecken, Ihr IT-Team beurteilen oder Einblicke in die Service-Desk-Exzellenz gewinnen? Dies erfuhr man in unserem Vortrag.

Vortragender: Jens Leucke (Freshworks, General Manager DACH)

AGENDA DER VERANSTALTUNG

IT-Strategien: Digitalisierung – Cloud – Daten und IT-Servicestrategie

Leitfaden zum Erstellen und Umsetzen einer erfolgreichen IT-Integrationsstrategie – Rahmenwerk, Roadmapping, Implementation, Governance
Ernst Tiemeyer (IT-Consultant)

Von Daten-Plattformen, Datenräumen und Daten-Ökosystemen. Moderne und verteilte Architekturen zum Data Sharing jenseits von zentralen (Cloud-) Datenbanken
Christoph F. Strnadl (Software AG)

IT Managed Services smart, sicher und individuell aufbauen – Ein Erfahrungsbericht der Modis IT Outsourcing GmbH aus dem komplexen Umfeld einer öffentlichen Verwaltung
Claudia Borst & Sven Lehmann (Akkodis)

Benchmarking: Wie gut ist Ihr IT-Service-Management? Wenn man es nicht messen kann, kann man sich nicht verbessern
Jens Leucke (Freshworks)

IT-Strategie zur Kundenzentrierung – ein Beitrag der Deutsche Bahn Cargo
Denyal Basaran (DB Cargo AG)

Security Trends: Cybersecurity – Artificial Intelligence – Sichere Architekturen

Cyber Security by Design: Angriffspfade in der Systemarchitektur erkennen, bevor es zu spät ist
Christoph Schmittner (AIT – Austrian Institute of Technology

Ransomware: sicher verschlüsselt! – Festplatte: verschlüsselt sicher?
Michael Strametz (SySS Cyber Security GmbH)

Cyber Defense in einem Unternehmen der kritischen Infrastruktur
Paul Mader, Florian Prack (Verbund)

IT-Strategie zur Kundenzentrierung

Denyal Basaran (DB Cargo AG)

Möchten Sie wissen, wie die IT-Strategie zur Kundenzentrierung der DB Cargo aussieht? Denyal Basaran sprach live in seinem Vortrag über die Herausforderungen, dem Einsatz und die Herangehensweise von Salesforce bei der @DB Cargo und gab darüber hinaus einen kurzen Ausblick.

Von Daten-Plattformen, Datenräumen und Daten-Ökosystemen. Moderne und verteilte Architekturen zum Data Sharing jenseits von zentralen (Cloud-) Datenbanken

Christoph F. Strnadl
(Software AG)

Über Daten-Plattformen, Datenräume und Daten-Ökosysteme, moderne und verteilte Architekturen zum Data Sharing jenseits von zentralen (Cloud-)Datenbanken« sprach Christoph F. Strnadl, Ph.D., CBPP von der Software AG!

Unternehmen tauschen seit den frühen 1990er Jahren (Stichwort: Electronic Data Interchange – EDI) höchst erfolgreich Daten aus – dies jedoch oft begrenzt auf lineare oder sehr hierarchische Wertschöpfungsketten. Der Einsatz von ein- oder mehrseitigen Plattformen durchbricht jedoch – etwa für Internet-of-Things-(IoT)-Anwendungsfälle — dieses strikte Punkt-zu-Punkt-Kommunikationsmuster (P2P) erstmals. Da diese Daten-Plattformen jedoch einen zentralen vertrauenswürdigen Intermediär voraussetzen, wurden diese Konzepte in den letzten 5–7 Jahren durch dezentralere Konzepte wie Datenräume und Datenökosysteme (bspw. Gaia-X) ergänzt. Vor dem Hintergrund von Praxisbeispielen vermittelte der Vortrag eine tragfähige Begriffsklärung (auch verwandter Begriffe wie Data Hub, Data Mesh u. a. m.), aktuelle IT-Architekturansätze und konkrete Handlungsempfehlungen, wie sich Unternehmen diesen strategischen Optionen nähern bzw. sie umsetzen können.

Die Veranstaltung wurde unterstützt von:

Sie wollen sich diese Vorträge nachträglich anschauen? Hier finden Sie weitere Informationen.

IT-Strategie

Leitfaden zum Erstellen und Umsetzen einer erfolgreichen IT-Integrationsstrategie – Rahmenwerk, Roadmapping, Implementation, Governance – Ernst Tiemeyer

Von Daten-Plattformen, Datenräumen und Daten-Ökosystemen. Moderne und verteilte Architekturen zum Data Sharing jenseits von zentralen (Cloud-)Datenbanken – Christoph F. Strnadl

IT Managed Services smart, sicher und individuell aufbauen – Ein Erfahrungsbericht der Modis IT Outsourcing GmbH aus dem komplexen Umfeld einer öffentlichen Verwaltung – Sven Lehmann, Claudia Borst

Benchmarking: Wie gut ist Ihr IT-Service-Management? Wenn man es nicht messen kann, kann man sich nicht verbessern – Jens Leucke

IT-Strategie zur Kundenzentrierung – Denyal Basaran

Security-Trends

Cyber Security by Design: Angriffspfade in der Systemarchitektur erkennen, bevor es zu spät ist – Christoph Schmittner

Ransomware: sicher verschlüsselt! – Festplatte: verschlüsselt sicher? – Michael Strametz

Cyber Defense in einem Unternehmen der kritischen Infrastruktur – Paul Mader, Florian Prack (Verbund)

CON•ECT Experience

Auf unserer Plattform CON•ECT Experience finden Sie außerdem einige Videos und Papers zu den verschiedensten Technologiethemen von zahlreichen Anwenderunternehmen und Forschungsinstituten wie Erste Group, Wien Energie, Deutsche Bahn, ABC Research etc.

Weitere interessante Beiträge und Videos finden Sie hier.

Wer ist das Future Network?

Das Future Network ist eine neutrale Plattform für EntscheiderInnen aus der Wirtschaft und Wissenschaft mit dem Fokus auf IT-Themen. Seit der Gründung im Jahr 1997 verknüpfen wir Technologie und Business für die zukunftsorientierte und praktische Umsetzung im Alltag. Mit der Expertise von über 500 internationale ExpertInnen spannt das Future Network einen Bogen von der anwendungsorientierten Forschung bis zur Praxis. Weiters bietet das Future Network Cert Zertifizierungen in den Bereichen »Requirements Engineering« und »Software Architecture«.

CON•ECT Business Academy

Die CON•ECT Business Academy bietet Ihnen hochkarätige Events, zertifizierte Ausbildungsprogramme, Seminare und Workshops mit Topspeakern aus Österreich, Deutschland und der Schweiz. Dabei legen wir besonderen Wert auf die Verbindung von Business- und IT-Themen.

CON•ECT Informunity

Bei der CON•ECT Informunity bieten wir Ihnen dort die Möglichkeit, hochaktuelle Themen und/oder Erfahrungen zu neuen Technologien und wirtschaftliche Entwicklungen kennenzulernen. Dazu gehört auch ein intensiver Erfahrungsaustausch mit unserem Netzwerk an AnwenderInnen, AnbieterInnen und ExpertInnen.