Einzelheftpreis € 15,-

6/2014

Februar April Juni August Oktober **Dezember**

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

„Industrie-IT: Die Gefahr kam mit der Vernetzung!"

Im Interview: Mario Emig, Head of Information Security Business Development bei Controlware

Mobile Security
- Mobile Application Management
- Einfaches VPN für mobilen Remote Access
- Interview mit Aruba: Enterprise Mobility Management

Security Management
- Risikomanagement im Zeitalter von Advanced Persistent Threats
- Lokale Adminrechte sinnvoll einschränken
- IAM goes Business Intelligence

Events, Trends und Technik
- IT im Katastrophenschutz: ENSURE-Projekt
- Informationsdienst für IT-Sicherheit als App
- Interaktive Visualisierung im Dienste der Security

DATAKONTEXT

www.datakontext.com

Interview mit Mario Emig,
Chef der Information Security bei Controlware

"Industrie-IT – die Gefahr kam mit der Vernetzung!"

Als einer der führenden unabhängigen und international agierenden Systemintegratoren unterstützt Controlware seit Gründung im Jahr 1980 seine Kunden mit Komplettlösungen und Dienstleistungen in der Informationstechnologie. Dabei verfolgt das Unternehmen den Grundsatz, die spezifischen Problemstellungen seiner Kunden in den Mittelpunkt all seiner Projekte zu stellen. Im Interview mit IT-SICHERHEIT verrät Mario Emig, Head of Information Security und Business Development bei der Controlware GmbH, wieso Security für Controlware ein zentrales Thema ist, wie es zur Entstehung des Controlware Security Day kam und welche Gefahren in industriellen Netzen im Rahmen von "Industrie 4.0" lauern, beziehungsweise wie diesen begegnet werden kann.

ITS: Die Bedeutung des Themas Security für Controlware scheint immens zu sein – immerhin hielten Sie vergangenen September bereits im sechsten Jahr in Folge Ihren Controlware Security Day ab. Wie kam es eigentlich dazu, eine solche Veranstaltung zu starten?
Mario Emig: Tatsächlich liegt die erste Veranstaltung sechs Jahre zurück. Controlware gehörte schon zum damaligen Zeitpunkt zu den Top-Systemintegratoren, auch im Bereich Informationssicherheit. Was auch diverse Awards von unseren Herstellern unterstreichen. Bereits seit mehr als 20 Jahren vertrauen uns namhafte Kunden aus allen Branchen ihre Security-Projekte an. Auch Landes- und Bundesbehörden arbeiten vertrauensvoll mit unseren Security-Experten zusammen. Unser Leistungsspektrum reicht von der Planung über die Implementierung – auf Kundenwunsch auch bis zum Managed Security-Betrieb.
Trotz oder gerade wegen diesen Erfolgen suchten wir vor sechs Jahren nach einer Möglichkeit, noch enger mit unseren Kunden zu kommunizieren. Gleichzeitig wollten wir eine Plattform schaffen, die es den Kunden ermöglicht, sich auch untereinander auszutauschen. Relativ schnell entstand dann das Konzept, einer zweitägigen Veranstaltung mit einem Programm, das sich unsere Kunden größtenteils selbst zusammenstellen können. Durch die begleitende Ausstellung mit über 20 unserer Partner haben die Kunden auch direkten Kontakt zu den Security-Herstellern.
Jetzt komme ich zu dem, was Controlware aus meiner Sicht zu einem besonderen Arbeitgeber macht. Nach der Vorstellung des Konzepts ´Controlware Security Day´ bei der Geschäftsführung gab es sofort grünes Licht. Damit war der Startschuss für das Projektteam gefallen, den Security Day zu planen.

ITS: Der Erfolg gibt Ihnen offenbar Recht –- mir persönlich schien es in diesem Jahr so, als ob die Kapazitäten in Ihren Räumlichkeiten an ihre Grenzen kommen. Worin liegt das Erfolgsrezept? Hat sich das Konzept im Laufe der Zeit verändert?
Mario Emig: Vielleicht ist das unser Erfolgsrezept: Wir haben das ursprüngliche Konzept bisher nur an wenigen Stellen angepasst. Unsere Kunden wissen genau, was sie erwartet und schätzen dies. Was die Frage nach der Kapazität angeht, ist es so, dass wir seit mehreren Jahren immer ausgebucht sind. Wir haben sogar das Luxusproblem einer Warteliste.

ITS: Wenn der Zuspruch weiterhin so wächst, müssen Sie nächstes Jahr wohl eine Entscheidung treffen: Teilnehmerzahl deckeln oder Räumlichkeiten wechseln.

Mario Emig: Natürlich gibt es auch Stimmen, die Veranstaltung an einen Ort mit größeren Kapazitäten zu verlegen. Für die, die die Räumlichkeiten von Controlware nicht kennen, muss man ergänzen, dass die Veranstaltung im Nachbargebäude des Controlware Firmensitzes, im wunderschönen Atrium unserer Schulungstochter ExperTeach, beziehungsweise in deren Schulungsräumen stattfindet. Besonders die Kunden, die aus den entfernteren Teilen unserer Republik anreisen oder auch unsere Kunden aus Österreich lernen so Controlware besser kennen. Wir bieten jedes Jahr auch eine Führung durch das Controlware Gebäude an, die jedes Mal reichlich in Anspruch genommen wird. Hier zeigen wir unter anderem unser Customer Service Center, von wo aus wir unsere sicheren und hochverfügbaren Managed Network-, Managed Security- und Managed Data Center-Services für mittelständische und Großunternehmen aus ganz Deutschland anbieten.

ITS: Welche Pläne haben Sie sonst mit dem Security Day? Gibt es Dinge, die Sie künftig verändern wollen?
Mario Emig: Wie bereits erwähnt, gibt es wenig Anlass an der Veranstaltung grundsätzliche Änderungen vorzunehmen. Allerdings wird es auch immer kleinere Anpassungen geben. Aber lassen Sie sich überraschen, welche das im nächsten Jahr sein werden. Der Termin steht jedenfalls bereits fest: der siebte ´Controlware Security Day´findet am 01. und 02. Oktober 2015 statt.

ITS: Kommen wir zu einem Thema, das Sie auch auf dem Presse-Roundtable am Vorabend des Security-Day auf die Agenda gesetzt hatten: IT-Sicherheit im industriellen Umfeld –- oder wie es neudeutsch heißt –- im Lichte von Industrie 4.0. Ist Industrial Security für Controlware tatsächlich ein Thema?
Mario Emig: In der Tat ist Industrial Security ein Thema für Controlware. Wir waren bereits 2008 mit einem eigenen Stand auf der SPS/IPC/DRIVES – eine mit rund 50.000 Besuchern und 1.300 nationalen und internationalen Ausstellern die deutsche Leitmesse für elektrische Automatisierungstechnik und integrierte Automatisierungslösungen – vertreten. Seit diesem ersten Messeauftritt bis heute konnten wir in konkreten Projekten eine Menge Erfahrungen sammeln.

ITS: Welche Gefahren sehen Sie durch die mit Industrie 4.0 einhergehende IT-Hochrüstung in der Produktion? Und was genau ist hier anders als in einer Office-Umgebung?
Mario Emig: Zunächst kann man sagen, dass es eine Menge Gemeinsamkeiten in Produktions- und Office-Umgebungen gibt: Auch in Produktionsnetzwerken wird immer öfter Ethernet und TCP/IP als Basis genutzt. Letztendlich geht es in beiden Umgebungen um den Schutz von Daten, also von geistigem Eigentum. Es gibt jedoch auch erhebliche Unterschiede. In der Produktion steht zunächst die Verfügbarkeit der Anlagen absolut im Vordergrund. Wenn sie sich die Taktfrequenzen anschauen, in denen beispielsweise ganze Autos entstehen oder Motoren zusammengesetzt werden, wird schnell klar, was es bedeutet, wenn eine solche Produktion auch nur für wenige Minuten oder Stunden ausfällt. In Office-Umgebungen steht dagegen meist die Vertraulichkeit ganz oben. Gefährdungspotential gibt es in beiden Umgebungen reichlich. Bei Industrienetzen wäre nur exemplarisch zu nennen: Anbindung von Automatisierungsnetzen an IT-Netzwerke und an das Internet zu Fernwartungszwecken, vermehrter Einsatz offener Standards und PC-basierter Systeme, Zugriffsverletzungen durch Dritte, Spionage und Manipulation sowie Datenverlust durch Malware.

ITS: Warum wurde Security für die Bereiche ´SCADA & Co.´ lange Zeit so vernachlässigt?
Mario Emig: Vor etwa 20 Jahren, als diese Systeme erstmals in Betrieb gingen, war Sicherheit noch kein Thema. Außerdem hatten viele dieser Systeme auch keine Verbindung zum Internet oder zu LANs. Physische Isolation gewährleistete damals die Sicherheit am besten.
Mit den Jahren hat sich auch die Aufgabenstellung an die Systeme verändert und damit einhergehend auch deren Konfiguration. Ein System, auf das früher lediglich ein einziger Computer neben einem Förderband Zugriff hatte, kann heute ohne große Mühe über das Internet erreicht werden.

ITS: Wenn es dem großen Heer an Security-Anbietern schon im Office-Sektor nicht wirklich gelingt, zuverlässig für Sicherheit zu sorgen, warum sollte es nun im industriellen Umfeld anders sein?
Mario Emig: Sagen wir es mal so: in unseren Projekten stehen nicht unbedingt die Hersteller x oder y im Vordergrund, vielmehr zählen hier organisatorische Aspekte. Wo liegen die Verantwortlichkeiten? Was ist in einem Krisenfall zu tun? Diese und ähnliche weitere Fragen sind da wichtig. Dabei muss man sagen, dass auch die Hersteller ihre Hausaufgaben gemacht haben. Hier hat sich eine Menge getan. Vor zwei bis drei Jahren war es noch die Bauweise der Sicherheitssysteme in Produktions-Umgebungen, die sich von der in Office-Umgebungen unterschied. Ich denke hier beispielsweise an Firewalls mit Hutschiene-Montage, die höheren Temperaturschwankungen ausgesetzt werden können und den harten Bedingungen in Produktionshallen angepasst wurden. Hier gibt es übrigens auch Standards, die man bei der Produktauswahl, je nach Szenario beachten sollte, zum Beispiel den Standard IEC-61850-3.

Neben der Bauweise sind es heute zusätzlich vor allem Protokolle, die Berücksichtigung finden. In Industrie-Umgebungen finden Sie oftmals komplett andere Protokolle als in Office-Umgebungen, wie DNP3, Modbus oder auch ICCP. Die Sicherheitssysteme, die dort eingesetzt werden, sollten natürlich auch die dort verwendeten Protokolle verstehen.

ITS: Das Schadenspotenzial einer manipulierten IT ist, wenn ich Sie recht verstehe, im industriellen Umfeld noch weit höher als in einer Büroumgebung. Was glauben Sie tun zu können, damit Firmen ihre Industrienetze sicher bekommen?
Mario Emig: Ich würde sagen, dass bei einem Produktionsstillstand die Auswirkungen direkt sichtbar werden. Bei Datendiebstahl sind die potentiellen Schäden aber sicherlich vergleichbar hoch. Lösungsansätze sind mehrdimensional: Gute Beratung muss im Vordergrund stehen und was dann rauskommt, sind sehr unterschiedliche Lösungen. In einem Fall reichen unter Umständen organisatorische Maßnahmen, in anderen Fällen gilt es, die bedrohten Umgebungen zu segmentieren. Auf jeden Fall sollte aber sicherheitstechnisch eine saubere Trennung von Office und Produktion stattfinden. Zugriffsregelungen sollten klar strukturiert sein und auch technisch durchgesetzt werden. Hier ist insbesondere der Wartungszugriff von Dritten zu nennen. Ratsam ist es, diese Zugriffe zudem genauestens zu protokollieren.

ITS: Gibt es bei Controlware schon konkrete Projekte im Zusammenhang mit industrieller IT? Wie sind ihre Erfahrungen?
Mario Emig: Es gibt eine Menge Projekte im Bereich industrieller IT. Aktuell arbeiten wir besonders eng mit Energieversorgern zusammen, aber auch die von mir erwähnten Erfahrungen aus Produktionsumgebungen stammen aus konkreten Projekten. Hier wurde unser Emergency Response Services Team (ERT), mit dem wir schnelle und zuverlässige Unterstützung bei IT-Sicherheitsvorfällen bei Notfällen anbieten, zu Einsätzen gerufen, wenn beispielsweise Produktionsanlagen durch Conficker zum Stillstand gebracht wurden.

Oft kommt uns zu Gute, dass wir nicht nur Security-Dienstleitungen anbieten, sondern unsere Kunden ganzheitlich beraten und unsere ganze Erfahrungen aus dem Themenbereich Netzwerke einbringen. Wir sind als Systemintegrator in der Lage, die komplette Umgebung unserer Kunden zu betrachten – nur so kann eine wirkungsvolle Security erzielt werden.

ITS: Vielen Dank für das Gespräch!

Das Interview führte Stefan Mutschler, stellvertretender Chefredakteur IT-SICHERHEIT