2. GAMP® Konferenz Cyber Security

Die Abwehr vorbereiten

"Wenn es ein Notfall ist, ist es schon zu spät." (Talleyrand)

3. Dezember 2020

online

ISPE | Gamp Community of Practice (COP) GAMP D-A-CH

Schwerpunktthemen:

- Cybersicherheit: Vom Angriff bis zur Spurensicherung
- Betriebskontinuität und Disaster Recovery planen
- IT / OT: Operation und Monitoring für die Cybersicherheit

GAMP

Eine Gemeinschaftsveranstaltung von
ISPE, APV, Concept Heidelberg und VDI/VDE-GMA

ISPE Germany | Austria | Switzerland Affiliate · APV · Concept Heidelberg · VDI VDE

GAMP®

Hintergrund

Eine wirksame und durchgängige Vorbereitung ist die Voraussetzung, um Cybersicherheitskonzepte effizient zu implementieren. Dabei sollte es nicht allein um IT-Schutzmaßnahmen und schnelle Recovery-Prozeduren gehen. In der Tat stellt die Spurensicherung eine wesentliche Aktivität der Cybersicherheit dar. Diese Abklärungsmaßnahmen sollen sowohl dabei helfen, den Angriff und dessen Tragweite genau zu verstehen (und zu melden), um die Schutzmaßnahmen für die Zukunft zu verbessern, als auch Strafanzeige und Regresse zu ermöglichen.
Eine konsequente Auslegung einer Cybersicherheit-Strategie setzt voraus, dass die drei folgenden Dimensionen wahrgenommen werden:

- Spurensicherung zur Angriffszeit
- Ganzheitliche Planung der Betriebskontinuität
- Echtzeit-Monitoring, -alarmierung und -aufzeichnungen

Selbst wenn deren Tragweite und Besonderheiten unterschiedlich sein können, betrifft die Vielseitigkeit dieser Maßnahmen gleichermaßen die „reinrassige" IT wie die in der Produktion mit z. B. ihrer Prozessleittechnik (Automation; OT).

Zielgruppe

Verantwortliche aus der pharmazeutischen Industrie für IT-Systeme, deren GMP-Compliance und Security. Entwickler und Entscheider der Gerätezulieferer für Produktion und Qualitätskontrolle.

Programm

Donnerstag, 3. Dezember 2020 *09.00-17.00 h*

Begrüßung/Einführung
Yves Samson, Kereon AG
Eberhard Klappauf, Klappauf-IT-Consulting

Cybersicherheit: Vom Angriff bis zur Spurensicherung

Die Fähigkeit, die Ursachen sowie die Tragweite eines Vorfalls zu verstehen, stellt einen wesentlichen Bestandteil der Problemlösung und des Verbesserungsprozesses (CAPA) dar. Dabei sind vollständige Spuren unerlässlich.

Aktuelle IT- / OT-Gefahren und Angriffe

- Aktuelle Vorfälle und ihre Charakteristika
- Überblick über die aktuellen Standards und meldenden Organisationen

Benjamin Honisch, Bundesamt für Sicherheit in der Informationstechnik (BSI)

A: Wie können Behörden unterstützen?

- BSI: Forderungen und Unterstützung

Benjamin Honisch, Bundesamt für Sicherheit in der Informationstechnik (BSI)

B: Wie können Behörden unterstützen?

- BKA / LKA: Forderungen und Unterstützung

N.N.

C: Erwartungen der GxP Aufsichtsbehörde hinsichtlich Cybersicherheit

- Cybersicherheit in der Inspektion & Annex 11

Yves Samson, Kereon AG

Betriebskontinuität und Disaster Recovery planen

Während bei einem Cyber-Angriff die Managementerwartungen auf eine möglichst rasche Wiederaufnahme des Betriebs zielen, sollten die Recovery-Maßnahmen die Spurensicherung nicht verhindern. Die Planung der Betriebskontinuität und der Disaster Recovery muss den Widerspruch zwischen Sicherung und Schnelligkeit lösen, so dass die Spurensicherung kein Hindernis für die Wiederaufnahme des Betriebs darstellt.

Forensik:
Maßnahmen der Spurensicherung und Rechtsverfolgung

- Warum Forensik ?
- „live-response"- / „post-mortem"-Analyse
- Aktueller Schadensumfang, Rechtsverfolgung
- Stilllegungs- / Wiederherstellungsmaßnahmen (Daten, Anwendung, Netz)

Die Essentials der Cyber-Abwehr (eine ultimative Prüfliste)
- Branchenneutral & branchenspezifisch
- Ungenügende Maßnahmen und Schwachstellen
- Die ultimative Prüfliste zur Erstversorgung

Betriebskontinuität und Notfallpläne gegen Cyber-Angriffe
- Definition:
  Betriebskontinuität vs Wiederherstellung (IT / OT)
- Planen der Betriebskontinuität & des Disaster Recovery
- Schnellstmögliches Recovery vs Beweissicherung und Angriffsspuren
- Personen, Funktionen, Rollen, Prozesse
- Maßnahmen

IT / OT: Operation und Monitoring für die Cybersicherheit

Die Schärfe und die Reaktionszeit eines Monitoringsystems sind für den aktiven Schutz einer IT Infrastruktur ausschlaggebend. Zusätzlich können Aufzeichnungen der Aktivitäten (Logs), die vor einem Cyber-Angriff stattgefunden haben, wichtige Hinweise zum Verständnis der Angriffsstrategie und der möglichen Ausdehnung der Gefährdung liefern.

Die aktuelle Entwicklung der IT und OT, mit einem „Ineinanderwachsen" dieser beiden Disziplinen, führt dazu, dass die Monitoringstrategien, die bisher fast ausschließlich für die IT angewendet worden sind, jetzt ebenfalls für die OT (Prozessleittechnik) eingesetzt werden sollten.

Maßnahmen für die IT
- IT-Infrastrukturen pro-aktiv und sicher betreiben und überwachen, SOC-IT
- IT-Monitoring: als Schlüsselkomponente der IT-Sicherheit und Verfügbarkeit,
- Vorbereitungen, Übungen, Reaktionszeiten, Kommunikation, ...

Maßnahmen und Besonderheiten für die OT
- OT-Infrastrukturen pro-aktiv und sicher betreiben und überwachen, SOC-OT
- OT-Monitoring: als Schlüsselkomponente der IT-Sicherheit & Verfügbarkeit
- Vorbereitungen, Übungen, Reaktionszeiten, Kommunikation, ...

Abschlussdiskussion / Schlusswort

Änderungen und Programmanpassungen vorbehalten

"Es kommt nicht darauf an, die Zukunft vorauszusagen, sondern darauf, auf die Zukunft vorbereitet zu sein. (Perikles, ca. 500 – 429 v.Chr.)."

Referenten

Thomas Balint, Siemens AG

Herr Thomas Balint ist seit Januar 1998 bei der Siemens AG tätig. Zunächst war er als Senior Consultant in der Siemens Kommunikation verantwortlich für die Unterstützung des Aufbaus des Netzwerk- und Sicherheitsgeschäfts mit Unternehmenskunden.
Herr Balint bekleidet derzeit die Position des Leiters für die Bereitstellung und Mobilisierung von Cyber-Sicherheitsdiensten in Digital Industry Customer Service. Er ist verantwortlich für die Leitung eines Expertenteams, das sich auf regionale Unterstützung, Einführung, Markteinführung, Beratung und technische Verkaufsunterstützung für Cyber-Sicherheitsdienste weltweit konzentriert.
Er verfügt über 20 Jahre Erfahrung in den Bereichen Cybersicherheit, Internetworking und Telekommunikation. Herr Balint hat einen Bachelor-Abschluss in Betriebswirtschaft und einen Abschluss als zertifizierter Telekommunikations-ingenieur.

Benjamin Honisch, BSI

Herr Honisch hat im Jahr 2011 seine Diplomarbeit im Fach Biologie mit Fokus auf Materialwissenschaften abgeschlossen. Seit 2013 ist er im BSI im Bereich "Schutz Kritischer Infrastrukturen" tätig. Herr Honisch ist Hauptverantwortlicher für den Sektor Gesundheit und unterstützt das Nationale IT-Lagezentrum des BSI und CERT-Bund.

Dr. Eberhard Klappauf, Klappauf-IT-Consulting

Dr. Eberhard Klappauf wechselte nach Physik-Studium und Promotion am MPI für Biophysik in die Industrie mit Aufgabenfeldern wie medizinische Diagnostik, SW- und HW-Entwicklung und –Implementierungen und Einführung von QS-Systemen. Nach 16 Jahren beim IT-System- und Beratungshaus COMLINE AG, als Lead Consultant Pharma verantwortlich für die Beratungsschwerpunkte CSV und IT-Service Management nach ITIL®, gründete er 2015 das eigene Beratungsunternehmen, ergänzt um Medizintechnik und Healthcare. Beratungsgegenstand ist der Lebenszyklus computerisierter Systeme mit Requirements-Engineering, das Risiko Management und Auditierung sowie das regulatorische Umfeld. Er ist Mitglied in der APV-Fachgruppe IT und der GAMP® DACH SIG.

Ulrike Reuter, Sanofi-Aventis Deutschland GmbH

Frau Ulrike Reuter hat 1989 ihre Diplomarbeit an der TU Darmstadt im Fachbereich Maschinenbau mit Fokus auf die Thermische Verfahrenstechnik abgeschlossen. Seit diesem Zeitpunkt ist sie am Standort Höchst in Frankfurt tätig. Stationen waren Projektleiterin in der Anlagenplanung, Betriebsingenieurin und Leiterin der Technical Compliance bei der Sanofi. Seit 2016 ist sie u.a. IS Risk Managerin im Bereich der Insulin Fertigung bei Sanofi.

Yves Samson, Kereon AG

Yves Samson ist Gründer der Kereon AG, Basel. Er ist u.a. Mitglied des GAMP® Europe Steering Committees und für die französische Übersetzung des GAMP® 5 verantwortlich. Er ist Chair und Mitgründer von GAMP® Francophone. Innerhalb der ISPE ist er auch Mitglied von verschiedenen Arbeitsgruppen u.a. bezüglich Datenintegrität und IT-Infrastruktur.

Seminaranmeldung
per Fax +49 6221/84 44 34 oder unter www.gamp-dach.de

Datum

Kurs-Nr. 3219
2. GAMP® Konf. Cyber Security
am 3. Dez. 2020 09.00-16.30 h

Kurs-Nr. 3217
13. GAMP® 5 Konferenz
am 1. Dez. 2020 09.00-17.00 h
und am 2. Dez. 2020 09.00-16.30 h

Teilnahmegebühr

2. GAMP® Konf. Cyber Security 990 EUR*

13. Offizielle GAMP® 5 Konferenz
plus 2. GAMP® Konf. Cyber Security 2190 EUR*

*zzgl. MwSt.

inkl. elektronischer Teilnehmerunterlagen
Mitglieder von Behörden und Hochschulen erhalten auf die Teilnahmegebühr 50% Nachlass.

Anmeldung

CONCEPT HEIDELBERG
P.O. Box 10 17 64
D-69007 Heidelberg
Telefon +49(0) 62 21/84 44-0
Telefax 49(0) 62 21/84 44 34
E-Mail: info@concept-heidelberg.de
www.gamp-dach.de

Eine Rechnung/Anmeldebestätigung geht Ihnen zu.

Anmeldung
Sie können sich ganz einfach per Fax, E-Mail oder online anmelden. Wir bearbeiten Ihre Anmeldung umgehend und beraten Sie gern bei offenen Fragen.

Anmeldebestätigung
Nach erfolgreicher Anmeldung erhalten Sie von uns eine schriftliche Bestätigung.

Vor der Veranstaltung
Einige Tage vor Seminarbeginn erhalten Sie von uns einen „Reminder" mit allen wichtigen Eckpunkten Ihres Seminars (Uhrzeiten, Adressen etc.).

Nach der Veranstaltung
Ihre Teilnahme am Seminar wird Ihnen mit einem Zertifikat bestätigt. Um immer noch besser werden zu können, bitten wir Sie im Anschluss an das Seminar um Ihre Meinung.

Nachbereitung
Nach dem Seminar stehen wir Ihnen selbstverständlich auch weiterhin für Fragen, Anregungen und Kritik zur Verfügung.

Einwilligungserklärung Datenschutz

☐ Mit meiner Anmeldung erkläre ich mich einverstanden, dass APV / Concept Heidelberg meine Daten für die Bearbeitung dieses Auftrages nutzt und mir dazu alle relevanten Informationen übersendet. Ausschließlich zu Informationen über diese und ähnlichen Leistungen werden mich APV / Concept Heidelberg per Email und Post kontaktieren. Meine Daten werden nicht an Dritte weiter gegeben (siehe auch Datenschutzbestimmungen unter www.apv-mainz.de/impressum/datenschutz/) / www.gmp-navigator.com/datenschutz. Ich kann jederzeit eine Änderung oder Löschung meiner gespeicherten Daten veranlassen.

Titel, Vorname, Name *

Firmenname *

Straße und Nr./Postfach *

Abteilung

Postleitzahl und Ort *

Telefon

E-Mail-Adresse des Teilnehmers *

Bestell-Nr. oder abweichende Rechnungsadresse

Datum * Unterschrift *

*Pflichtangaben

☐ Anmeldung 2. GAMP® Konf. Cyber Security am 3. Dezember 2020
oder
☐ Anmeldung 2. GAMP® Konf. Cyber Security am 3. Dezember 2020
plus 13. Offizielle GAMP® 5 Konferenz, 1.-2. Dezember 2020