Mangelnde Informationssicherheit gefährdet die Patientensicherheit

Information Security in Health Conference, 22. Juni 2017

Christoph Knöpfel / Thomas Manser

Agenda

1. Die Bedrohungslage ist real
2. Einleitung zu Risikomanagement von Medizinprodukten in Netzwerken
3. Praxisbeispiel für eine mögliche Umsetzung in Zusammenarbeit mit der Medizintechnik
4. Fazit und Diskussion

WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

12.05.2017 17:59 Uhr – Martin Holland, Axel Kannenberg

vorlesen

Screensh

In ganz
lahmge
von Inf

In ganz
Angreif
freigeb

und Norden Englands betroffen. Die IT ist dort entweder wegen des Trojaners nicht mehr benutzbar, oder weil Rechner aus Vorsicht heruntergefahren wurden. Teilweise werden Patienten gebeten, nicht in die Notaufnahmen zu kommen, sondern nur Notrufnummern zu wählen. Der Nationale Gesundheitsdienst hat inzwischen erklärt,

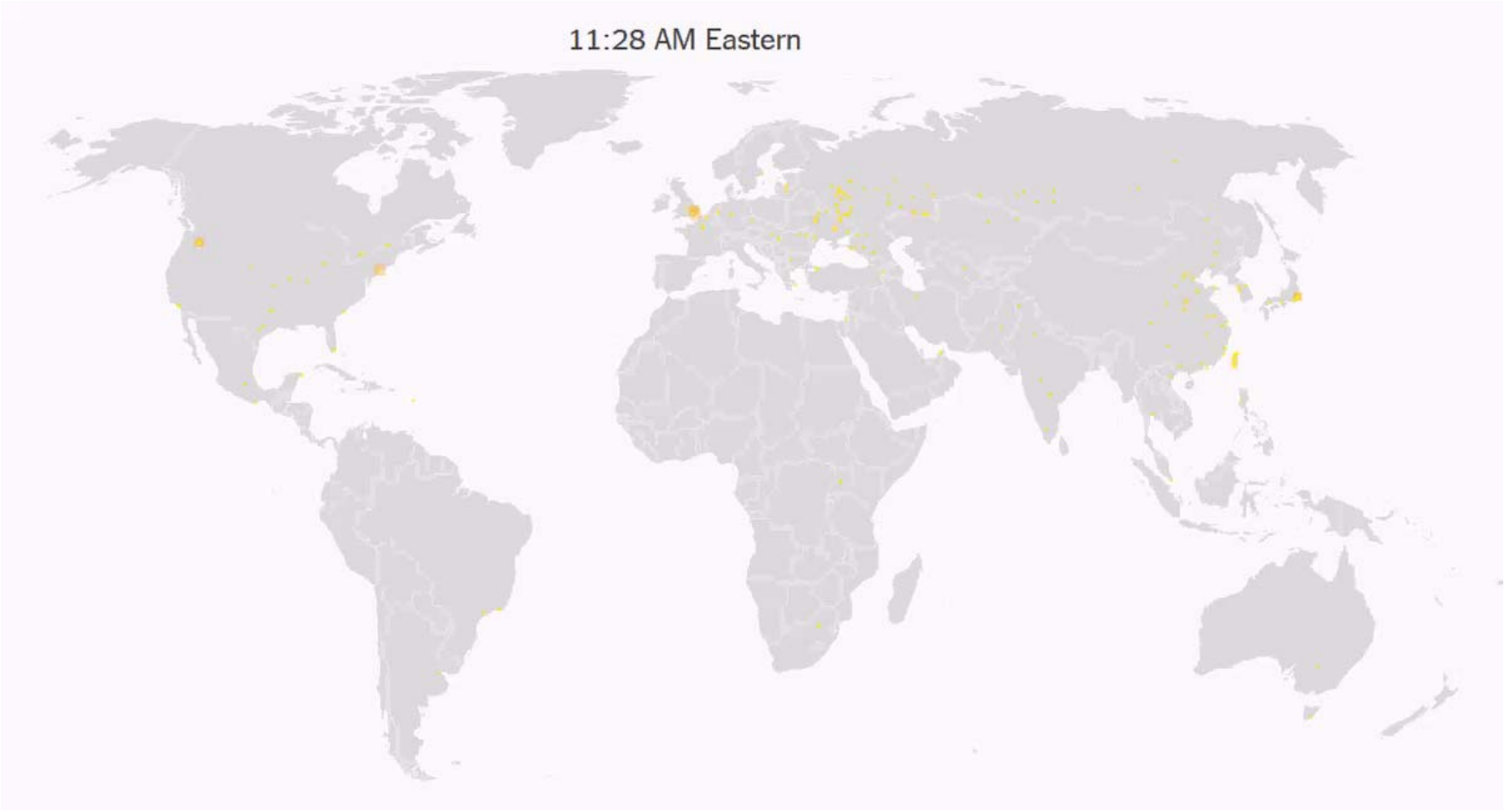
200'000 Nutzer von Cyberattacke betroffen

Die Polizeibehörde Europol spricht nach der Cyber-Attacke von einem Hackerangriff «bislang beispiellosen Ausmasses». Die erpresste Schadenssumme ist dagegen gering.

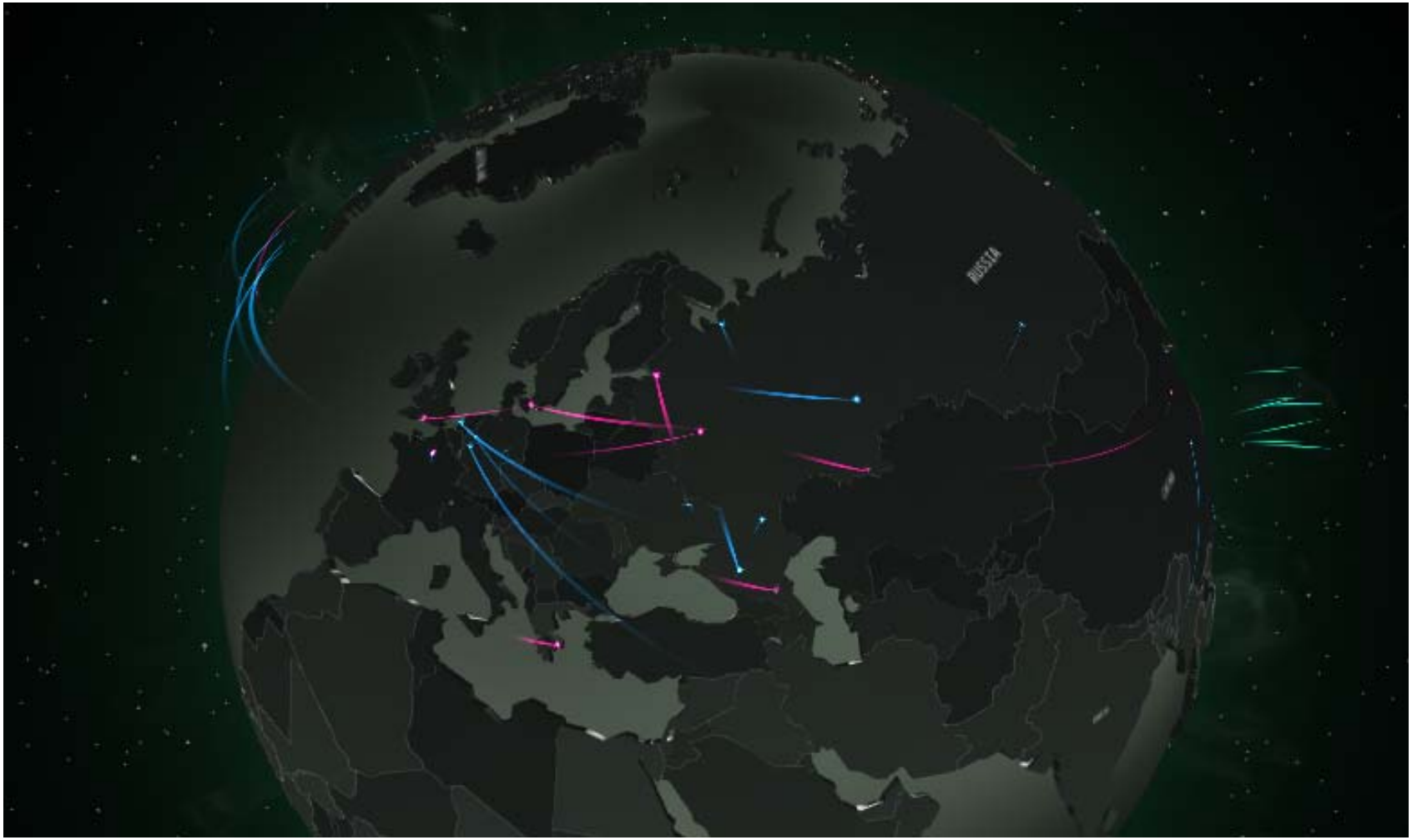
Im Falle des **Ransomware-Angriffs mit WannaCry** scheint klar: Die Cyberkriminellen sind gar nicht in der Lage, den individuellen Betroffenen einen Schlüssel zu liefern. Eine Bezahlung von **Lösegeld** ist also komplett sinnlos. Das zumindest sagt das Sicherheitsunternehmen Check Point.

computerworld.ch

Weltweite Infektion innert Stunden



7x24x365



Abhängigkeit Strom und Netzwerk

Montag, 20.03.2017 / 17:10 3

Panne legt IT der Stadt Zürich lahm (ergänzt)

Eine technische Panne hat am Montag einen grossen Teil der Informatik der Zürcher Stadtverwaltung sowie der Stadtspitäler Triemli und Waid lahmgelegt. Die Websites waren und sind (Stand 17.06) offline und konnten nicht aufgerufen werden. Auch etliche interne Dienste waren betroffen.

Wer die Stadtverwaltung über das Internet kontaktieren will, muss sich weiterhin gedulden. "www.stadt-zuerich ist zur Zeit nicht verfügbar. Wir bitten um Verständnis und freuen uns auf Ihren nächsten Besuch", hiess es während Stunden auf der Website.

Ursache der Störung war ein Defekt im Rechenzentrum Hagenholz, wie die Abteilung Organisation und Informatik (OIZ) mitteilte. In der Nacht sei eine zentrale Hardwarekomponente ausgefallen und dies habe dazu geführt, dass das Internet nicht mehr funktionierte, sagte OIZ-Sprecher Martin Otzenberger gegenüber 'sda'. Ein Hacker-Angriff könne auf jeden Fall ausgeschlossen werden.

Von der Informatik-Panne betroffen waren auch etliche Computerarbeitsplätze in der Verwaltung. In den Stadtspitälern Triemli und Waid konnten die Patienteninformationen nicht mehr abgerufen werden.

Dies führte laut Otzenberger beispielsweise dazu, dass Röntgenbilder nicht mehr am Bildschirm eingesehen werden konnten, sondern - wie früher - von Mitarbeitenden auf die einzelnen Abteilungen getragen werden mussten. Das habe zu Mehrarbeit geführt, die Patienten seien aber nicht gefährdet gewesen.

Einleitung zu Risikomanagement von Medizinprodukten in Netzwerken

Die Digitalisierung setzt sich kontinuierlich fort …

… mit allen Konsequenzen!

Risikomanagement von Medizinprodukten

Grundlagen

- IEC 80001-1 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
- Basierend auf der Europäischen Richtlinie MDD 93/42 EWG Medizinprodukterichtlinie
- Medizinprodukteverordnung 812.213 (MedV)des Bundes
- Diverse Standards für die Klassifizierung von Produkten oder deren Betrieb wie:
  - IEC 60601 Sicherheitsanforderungen an medizinische elektrische Systeme
  - ISO 14971 Anwendung des Risikomanagements auf Medizinprodukte
  - ISO 13485 Aufbau eines Qualitätsmanagementsystems
  - IEC 62304 Medizingerätesoftware – Softwarelebenszyklusprozesse
  - IEC 62366 Anwendung der Gebrauchstauglichkeit auf Medizinprodukte

Risikomanagement von Medizinprodukten

Definition eines Medizinproduktes gemäss MepV Art.1

Medizinprodukte sind einzeln oder miteinander verbunden verwendete Instrumente, Apparate, Vorrichtungen, Software, Stoffe, Zubehör oder andere medizinisch-technische Gegenstände, einschliesslich der speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinprodukts eingesetzten Software:

- die zur Anwendung beim Menschen bestimmt sind;
- deren bestimmungsgemässe Hauptwirkung im oder am menschlichen Körper nicht durch pharmakologische, immunologische oder metabolische Mittel erreicht wird, deren Wirkungsweise durch solche Mittel aber unterstützt werden kann; und
- die dazu dienen:
  - Krankheiten zu erkennen, zu verhüten, zu überwachen, zu behandeln oder zu lindern,
  - Verletzungen oder Behinderungen zu erkennen, zu überwachen, zu behandeln oder zu lindern oder Behinderungen zu kompensieren,
  - den anatomischen Aufbau zu untersuchen oder zu verändern, Teile des anatomischen Aufbaus zu ersetzen oder einen physiologischen Vorgang zu untersuchen, zu verändern oder zu ersetzen,
  - die Empfängnis zu regeln oder Diagnosen im Zusammenhang mit der Empfängnis zu stellen.1

Risikomanagement von Medizinprodukten

Klassifikation von Medizinprodukten gemäss MepV Art.5

- Klasse I:
  - Eigenschaften: Keine methodischen Risiken, geringer Invasivitätsgrad, kein oder unkritischer Hautkontakt, vorübergehende Anwendung ≤ 60 Minuten
  - Beispiel in Bezug auf die Informationssicherheit: Software zur integrierten Versorgung
- Klasse IIa:
  - Eigenschaften: Anwendungsrisiko vorhanden, mässiger Invasivitätsgrad, kurzzeitige Anwendung im Körper, kurzzeitig ≤ 30 Tage
  - Beispiel in Bezug auf die Informationssicherheit: PACS ohne Strahlentherapie
- Klasse IIb:
  - Eigenschaften: Erhöhtes methodisches Risiko, systematische Wirkung, Langzeitanwendung, langzeitig ≥ 30 Tage
  - Beispiel in Bezug auf die Informationssicherheit: PACS mit Strahlentherapie
- Klasse III
  - Eigenschaften: Besonders hohes methodisches Risiko, langfristige Medikamentenabgabe, unmittelbare Anwendung an Herz, zentralem Kreislaufsystem oder zentralem Nervensystem

Die Bestimmung der Klasse liegt in der Verantwortung des Herstellers.

Anwendungsbeispiel von IEC 80001-1

Gerade im Bereich der Vernetzung von IT-Komponenten besteht häufig bei den Betreibern von Medizinprodukten eine Diskrepanz zwischen der Informatik und der Medizintechnik.

Diese Diskrepanz kommt häufig erst zum Vorschein, wenn ein Informationssicherheits-Ereignis im Netzwerk vorliegt oder – wie erst kürzlich - innert kürzester Zeit ein Security Patch für Betriebssysteme eingespielt werden muss.

Möglicher Ansatz für eine Bestimmung der Verantwortlichkeiten

Bestimmung von Kategorien der anzuschliessenden Komponenten:

- Kat 1: Standard Arbeitsplatz (AP)
  - Full-Service durch IT, inkl. Malwareschutz, Applikationen die über die Softwareverteilung verwaltet werden können
- Kat 2: Spezifische Anwendung auf Standard AP mit Abhängigkeiten zum Betriebssystem:
  - Unterscheidung zu Kat. 1; Service (insb. Updates) nur in Abstimmung mit Lieferant (zwingend)
  - Fachapplikation wird durch Lieferant direkt installiert und durch einen Fachbereich ausserhalb der IT (z.B. Medizintechnik) verwaltet
- Kat 3: Hardware und Anwendung vom Lieferanten, einzelne Subservices durch IT (Betriebssystem, Malwareschutz, E-Mail, usw.):
  - Betrieb erfolgt in Abstimmung (insb. Updates) mit dem Lieferant (zwingend) und dem zuständigen Fachbereich
  - Achtung: Wartungsvertrag prüfen inwiefern alle Dienstleistungen enthalten sind
- Kat 4: Blackbox vom Lieferant, mit Netzwerkzugang, Full-Service durch Lieferant:
  - Kompletter Betrieb muss vom Lieferanten in Abstimmung mit den zuständigen Fachbereich gewährleistet werden

Möglicher Ansatz für eine Bestimmung der Verantwortlichkeiten

Insbesondere für Kat. 3 und 4 Komponenten ist die Einteilung der Netze nach EN 60601 zu beachten (A=normales Netz, B=eigenes VLAN, C=Hardware gekapseltes Netz)

Konsequenz	Reaktions-zeit	Netz	Beispiele
Tod, schwerwiegende Patientenschädigung	Sekunden	C	Fehlverhalten durch Infusionspumpen, Operationsroboter
	Minuten	C	Übertragung von Alarmen, die am Bett unterdrückt werden
	Stunden	C/B	Überwachungsdaten eines Beatmungsgerätes
Mittlere Patientenschädigung	Sekunden	C	Generelle Kommunikation zu Infusionspumpen und Operationsroboter
	Minuten	C/B	Generelle Kommunikation zu Infusionspumpen und Operationsroboter
	Stunden	C/B	Verfälschung der Bildgebung
Leichte Patientenschädigung	generell	B	Kommunikationsverlust zu einem Gerät mit Röntgenstrahlen
Vernachlässigbare Patientenschädigung	generell	A	

Möglicher Ansatz für eine Bestimmung der Verantwortlichkeiten

Regelung der Verantwortlichkeiten

Services	Kat 1	Kat 2	Kat 3	Kat 4
Netzwerk (farbcodiert)	Full-Service IT	Full-Service IT	Full-Service IT in Abstimmung mit dem Lieferanten	In Abstimmung mit dem Lieferanten
Betriebssystem	Full-Service IT	Full-Service IT Wartung nach Rücksprache mit Lieferant	In Abstimmung mit dem Lieferanten	Lieferant
Malwareschutz	Full-Service IT	Full-Service IT Wartung nach Rücksprache mit Lieferant	In Abstimmung mit dem Lieferanten	Lieferant
Applikations-management	Full-Service IT	In Abstimmung mit dem Lieferanten	Lieferant	Lieferant

Konsequenzen aufgrund fehlender Verantwortlichkeiten

- In der Beschaffung von Medizinprodukten gehen wichtige Auswahlkriterien vergessen und die budgetierten Investitions- und Betriebskosten aus dem Investitionsantrag werden massiv überschritten.
- Medizinprodukte funktionieren nur noch eingeschränkt nach unkoordinierten Netzwerkarbeiten (Patches, Softwareupdates von Netzwerkkomponenten, Firewall Konfigurationen, …).

  => Gefährdung der Patientensicherheit je nach Medizinprodukte Klassifizierung
- Medizinprodukte funktionieren nur noch eingeschränkt (insbesondere Performancekriterien) nach unkoordinierten Wartungsarbeiten bezüglich Malwareschutz im Betriebssystem oder entsprechenden Services

  => Gefährdung der Patientensicherheit je nach Medizinprodukte Klassifizierung
- Die IT-Infrastruktur funktioniert nur noch eingeschränkt nach unkoordinierten Wartungsarbeiten durch den Lieferanten des Medizinproduktes

  => Gefährdung der Patientensicherheit je nach Medizinprodukte Klassifizierung

Fazit

- Die Bedrohung ist real und vermehrt wird das Gesundheitswesen in die Pressemitteilungen von Bedrohungslagen miteingebunden.
- Erst kürzlich durfte wegen der Schadsoftware «Wanna Cry» in vielen Spitälern umfangreiche Sicherheitsmassnahmen durchgeführt werden. Im Eilzugstempo wurden viele Microsoft Windows Betriebssysteme aktualisiert. Da blieb keine Zeit, noch lange bei den Herstellern von Medizinprodukten nachzufragen, inwiefern eine Aktualisierung der Betriebssysteme zulässig ist.
- Aus der aktuellen Bedrohung wurden somit viele Verantwortlichkeiten direkt vom Lieferanten zum Betreiber unbewusst übertragen. Falls durch eine Fehlfunktion eines Medizinproduktes oder fehlende Behandlungsdaten ein Patient geschädigt worden wäre, hätte die Verantwortung voll und ganz durch die entsprechende Institution getragen werden müssen.

Nehmen Sie die Bedrohung ernst und handeln Sie mit der Erarbeitung von klaren Zuständigkeiten im Bereich der Informationssicherheit!

Herzlichen Dank für Ihre Aufmerksamkeit

Thomas Manser

Direkt +41 71 231 10 74
Thomas.manser@csp-ag.ch

Christoph Knöpfel

Direkt +41 71 231 10 77
christoph.knöpfel@csp-ag.ch

CSP AG
Teufener Strasse 5
CH-9000 St.Gallen
Tel +41 71 231 10 60
www.csp-ag.ch