Angriff auf medizinische Infrastrukturen

Tagung Patientensicherheit - Aktueller Stand
Medizinische Hochschule Hannover

Agenda

- Vorstellung
- Risiken durch Cyberangriffe
- Angriffsmethoden auf Gesundheits-Infrastrukturen
  - Digitale Angriffswege
  - Physische Angriffswege
- Ideen zur Mitigation

Vorstellung

- Jan Felix Wiebe (clarity@hannover.ccc.de)
  - Mitglied Chaos Computer Club Hannover
  - Mitglied Arbeitsgemeinschaft Kritische Infrastrukturen
  - tätig im Bereich Informationssicherheit / Kritische Infrastrukturen
  - Prüfer für Kritische Infrastrukturen nach §8a BSIG
- Jan Schreiber (hans@hannover.ccc.de)
  - Mitglied Chaos Computer Club Hannover
  - tätig im Bereich Offensive Cyber Security
  - Weitere Schwerpunkte: Sichere Softwareentwicklung, Kryptografie

Chaos Computer Club Hannover

- Lose Gemeinschaft von technikinteressierten Menschen
- Clubräume in der Bürgerschule Stadtteilzentrum Nordstadt
- Chaos macht Schule: Zusammenarbeit mit Schulen und Bildungseinrichtungen zur Förderung d. Medienkompetenz
- Jährliche Veranstaltung: Hackover
- Informationen: https://hannover.ccc.de

Risiken durch Cyberangriffe

Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm

Der Albtraum jeder Klinikleitung: Malware legt die Systeme im Krankenhaus lahm. So geschehen ist das in mehr als zehn Häusern in Rheinland-Pfalz und Saarland.

Lesezeit: **2 Min.** In Pocket speichern 414

(Bild: plantic\Shutterstock.com)

17.07.2019 19:11 Uhr

Von dpa

Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm

Der Albtraum jeder Klinikleitung: Malware legt die Systeme im Krankenhaus lahm. So geschehen ist das in mehr als zehn Häusern in Rheinland-Pfalz und Saarland.

Lesezeit: **2 Min.** In Pocket speichern 414

(Bild: plantic\Shutterstock.com)

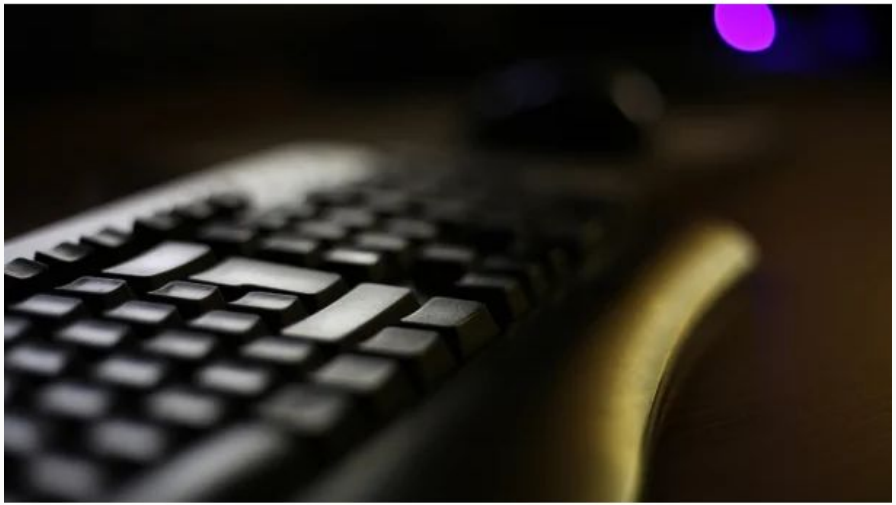
17.07.2019 19:11 Uhr

Von dpa

Cyber-Attacke auf Kliniken: Schwachstelle war "altes Dienstkonto"

Im Juli hatten Krankenhäuser und DRK-Einrichtungen in Rheinland-Pfalz und im Saarland mit Malware-Befall zu kämpfen. Nun ist das Einfallstor bekannt.

Lesezeit: **1 Min.** In Pocket speichern 35



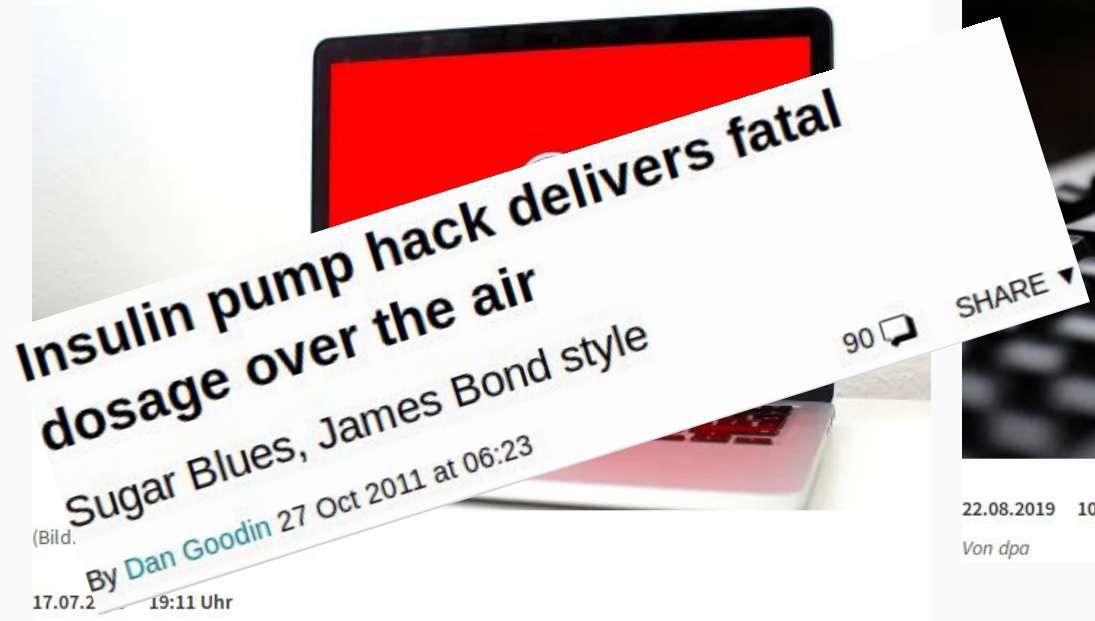
22.08.2019 10:53 Uhr

Von dpa

Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm

Der Albtraum jeder Klinikleitung: Malware legt die Systeme im Krankenhaus lahm. So geschehen ist das in mehr als zehn Häusern in Rheinland-Pfalz und Saarland.

Lesezeit: **2 Min.** In Pocket speichern 414



(Bild.

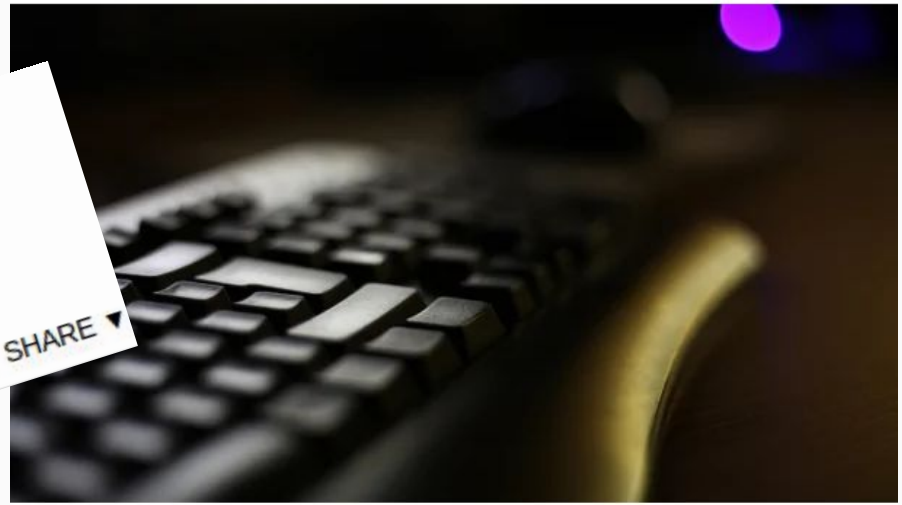
17.07.2 19:11 Uhr

Von dpa

Cyber-Attacke auf Kliniken: Schwachstelle war "altes Dienstkonto"

Im Juli hatten Krankenhäuser und DRK-Einrichtungen in Rheinland-Pfalz und im Saarland mit Malware-Befall zu kämpfen. Nun ist das Einfallstor bekannt.

Lesezeit: **1 Min.** In Pocket speichern 35



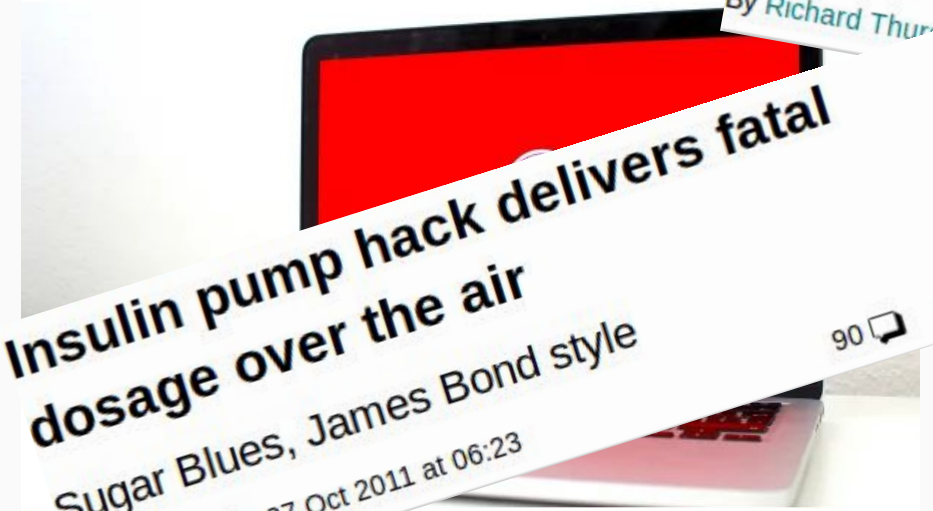
22.08.2019 10:53 Uhr

Von dpa

Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm

Der Albtraum jeder Klinikleitung: Malware legt die Systeme im Kran
lahm. So geschehen ist das in mehr als zehn Häusern in Rheinland
Saarland.

Lesezeit: **2 Min.** In Pocket speichern



(Bild.

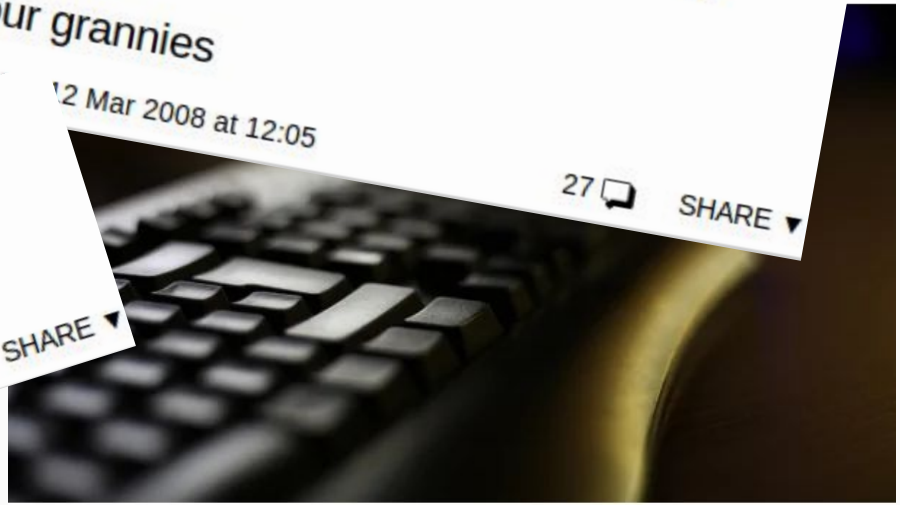
17.07.2 19:11 Uhr

Von dpa

Cyber-Attacke auf Kliniken: Schwachstelle war "altes Dienstkonto"

Krankenhäuser und DRK-Einrichtungen in Rheinland-Pfalz und im
fen. Nun ist das Einfallstor bekannt.

35



22.08.2019 10:53 Uhr

Von dpa

Hacking attacks can turn off heart monitors

Lock up your grannies

By Richard Thur

2 Mar 2008 at 12:05

27 SHARE

Insulin pump hack delivers fatal dosage over the air

Sugar Blues, James Bond style

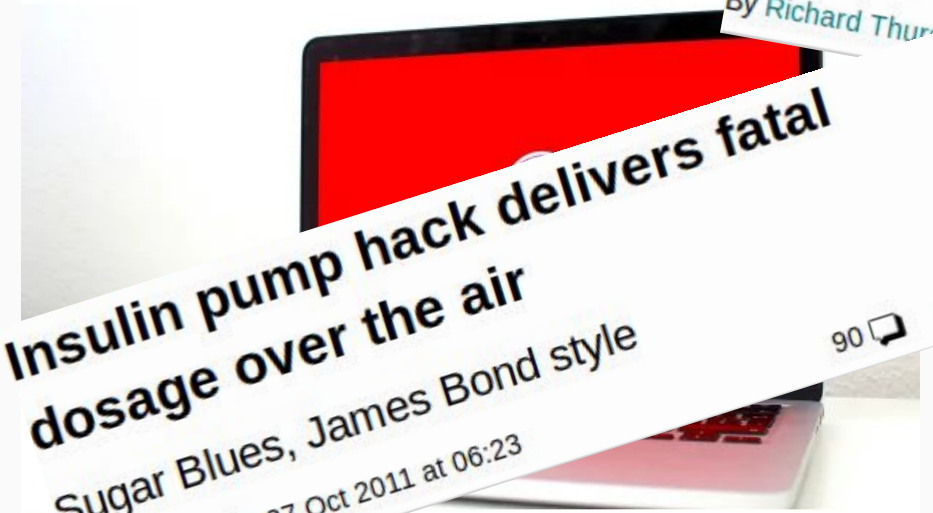
By Dan Goodin 27 Oct 2011 at 06:23

90 SHARE

Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm

Der Albtraum jeder Klinikleitung: Malware legt die Systeme im Kran
lahm. So geschehen ist das in mehr als zehn Häusern in Rheinland
Saarland.

Lesezeit: 2 Min. In Pocket speichern



(Bild.

17.07.2 19:11 Uhr

Von dpa

Cyber-Attacke auf Kliniken: Schwachstelle war "altes Dienstkonto"

Krankenhäuser und DRK-Einrichtungen in Rheinland-Pfalz und im
pfen. Nun ist das Einfallstor bekannt.

35

Hacking attacks can turn off heart monitors

Lock up your grannies

By Richard Thur

12 Mar 2008 at 12:05

Insulin pump hack delivers fatal dosage over the air

Sugar Blues, James Bond style

By Dan Goodin 27 Oct 2011 at 06:23

90

SHA

ÄrzteZeitung

Print
App
Newsletter

Politik | Krankheiten | Fachbereiche | Praxis & Wirtschaft | Panorama

Sie befinden sich hier: Home » Praxis & Wirtschaft » Digitalisierung und IT » Datenschutz

Ärzte Zeitung online, 22.11.2018

Klinikum Fürstenfeldbruck

Cyber-Attacke nur Zufall?

22.08

Von d

Ein Krankenhaus, in dem kein Computer funktioniert. Diese Erfahrung musste das Krankenhaus in Fürstenfeldbruck machen. Welche Folgen der Cyber-Angriff haben wird, ist noch nicht absehbar – auch für Praxen.

Von Joachim Jakobs

Cyberangriffe heute

- Cyberangriffe sind (leider) ein reales Risiko
- Vernetzung exponiert medizinische Geräte sowie Infrastruktur
- Nicht vergessen: Zutrittssysteme, Gebäudesteuerung, Notrufsysteme
- Medizinische Geräte sind auch nur Computer!
- Ansteuerbar über standard Protokolle
  - Bluetooth
  - (Wireless) Lan
  - Serielle Schnittstellen

Beispiel eines Angriffes

Reconnaissance

Erkundung und Informationssammlung

Exploitation

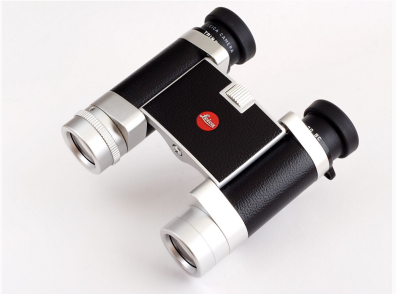
Ausnutzung der gefundenen Schwachstellen aus 1

Exfiltration

Extraktion von Informationen/Daten; Anrichten von Schaden

Reconnaissance

- Ausspähung des potentiellen Opfers
- Suche nach öffentlich Informationen
  - Webseite
  - IP Adressbereiche
  - Mitarbeiter auf Sozialen Medien
  - bereits bekannte Datenlecks
- Eingesetzte Geräte
  - Hersteller
  - Zulieferer



Exploitation

- Ausnutzung der gesammelten Informationen
  - veraltete Software
  - leichtgläubige Mitarbeiter
  - ungenügende Gebäudesicherheit
  - keine aktiven Erkennungsmechanismen für Angriffe aus dem Internet
- Beispiel: Verteilen von USB-Sticks mit Schadsoftware auf dem Parkplatz
  - auch direkt auf einer Station möglich
  - USB-Stick führt sofort Schadsoftware aus
  - öffnet dem Angreifer weitere Tore

Exfiltration

- Extraktion von Informationen
  - Usernamen
  - Passwörter
  - E-Mail Adressen
  - Patientendaten
- Anrichten schon Schaden
  - Verschlüsselungstrojaner
  - manipulation von Geräten
  - ändern von Patientendaten

Physische Angriffsszenarien

- Weitere Einfallswege neben technischen Zugriffen
  - Physikalische Sicherheit
    - Sicherheitsbereiche
    - Zutritt zu Computern, Netzwerkinfrastruktur und Servern
    - Zugang zu Patienten
  - Social Engineering
    - “CEO Fraud”
    - Als Familienmitglied ausgeben

Sicherheit - multiple Persönlichkeit?

Safety

Betriebssicherheit, Schutz von Mensch und Umwelt

Security

Schutz vor beabsichtigten, aber unberechtigten Zugriffen

Bei kritischen Infrastrukturen hat “security” einen direkten Einfluss auf “safety”!

Ideen zur Mitigation

- Ganzheitliche Sicherheit betrachten
- Zur Patientensicherheit gehört auch Informations- und IT-Sicherheit!
- Lassen sie ihre IT- und Informationssicherheit durch Dritte prüfen (Red Teaming)
- Nutzen sie Standards (ISO 27001, B3S) für Informationssicherheit

- Einstiegspunkt: “Schutz kritische Infrastruktur: Risikomanagement im Krankenhaus” des BBK

Vielen Dank!

Kontakt:

Jan Felix Wiebe
(clarity@hannover.ccc.de)

Jan Schreiber
(hans@hannover.ccc.de)

https://hannover.ccc.de