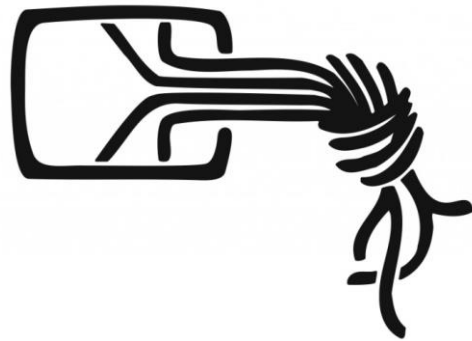


„Digitaler Leichtsinn“ im Krankenhaus



Martin Schobert <martin@berlin.ccc.de>

Über den Referenten

- im CCC seit 1998
- IT-Sicherheit, Softwareentwicklung, Administration
- Beruflich IT-Sicherheitsanalyst
 - Netzwerke, Hardware, Software
 - Papier, White-/Grey-/Blackbox
- Diverse Penetrationstests in Krankenhäusern, Diagnostikgeräte, Pharma

Themen

- Ausgangslage
- Sicherheitsprobleme als Industrie-Standard
- „Digitaler Leichtsin“
 - Vernetzung
 - Verantwortungsverteilung
 - Fragilität von Produkten
- Optional: Nicht nur die Cyber-Kriminellen ...
- Empfehlungen
- Diskussion

Ausgangslage

- Etwa 2000 Krankenhäuser in Deutschland
- öffentlich, privat und freigemeinnützlich
- Unterschiedliche Größe und Leistungsfähigkeit
- Ebenso bei der Krankenhaus-IT
- Technische IT-Sicherheit oft Zusatzaufgabe für Admins

Besondere Aspekte im Gesundheitswesen

- Krankenhaus-Mitarbeiter überwiegend ohne IT-Hintergrund
 - Geringe Akzeptanz für „Arbeitserschwerisse“
- Öffentlich zugängliche Einrichtungen
 - physisch
 - informationell
- Kostendruck, besonders auf die IT
- Gelebte Annahme: Wer wird denn ein Krankenhaus angreifen?

Sicherheitsprobleme als Industrie-Standard

- Alles ist eine Vertrauenszone
 - Flache Netzwerkstruktur ohne wirksame Einschränkungen
- Standard- und Trivialpasswörter
- Wartungszugänge
- Seltene oder keine Softwareupdates
- Klartextkommunikation

Vergessene und vernachlässigte Computer: Grundlegende Systeme

- Betriebsleittechnik
 - Wärme, Wasser, Luft, Gas, Strom
- Netzwerkinfrastruktur
- Telefonie

Vergessene und vernachlässigte Computer: Anwendungs- und Unterstützungsbereich

- Drucker
- WLAN
- Infotainment
- Parken, Kassensysteme, Videoüberwachung, Zutrittskontrolle, ...

Vergessene und vernachlässigte Computer: Anwendungs- und Unterstützungsbereich

- Tatsächlich vergessene Installationen (Server, Dienste)
- Systeme, die man nicht selbst betreibt

Vergessene und vernachlässigte Computer: Medizinalbereich

- Laboranalysegeräte
- Patienten-Monitoring
- Bildgebende Verfahren

Immer mehr Vernetzung ohne wesentliche Sicherheitsverbesserung

- Vergessene Systeme + Standardprobleme + an „erreichbaren Netzen“
- Zunehmend Online-Dienste (Cloud) für Arztpraxen und Endnutzer

Bis zur Auflösung verteilte Sicherheitsverantwortung

- Verteilte Sicherheitsverantwortung
 - Hersteller
 - IT-Leitung im Krankenhaus
 - Krankenhaus-interne Admins
 - Nutzer
 - Externe Wartung
- Niemand fängt das auf

Beispiel Betriebsleittechnik, Wasseraufbereitung, Gase, ...

- Geräte mit Standardpasswörtern im Krankenhausnetz mit Fremdzugriff und seltenen Updates

Beispiel Betriebsleitetechnik, Wasseraufbereitung, Gase, ...

- Geräte mit Standardpasswörtern im Krankenhausnetz mit Fremdzugriff und seltenen Updates
- Hersteller:
 - Kunde fordert keine Sicherheit ein
 - Keine Anforderung, Passwörter zu ändern
- IT-Leitung, IT-Admin:
 - keine IT, sondern Betriebstechnik
 - Keine besonderen Sicherheitsanforderungen, Geräte einzusperren
 - Passwort-Management macht Hersteller
- Technischer Nutzer: soll funktionieren, keine Erschwernis
- Externe Wartung: keine Sicherheitsvorgaben erhalten

Beispiel Betriebsleitetechnik, Wasseraufbereitung, Gase, ...

- Effekte:
 - Alle Kunden/Konkurrenten haben die gleichen Standard-Passwörter
 - Kein Prozess vorhanden, um
 - Passwörter regelmäßig zu wechseln
 - Passwörter zu dokumentieren und zu verwalten
 - Keine individuellen Accounts, keine sinnvollen Logs
 - Kein Nachdenken über Alternativen zu Passwörtern
- Krankenhaus ist KRITIS, damit auch die Building-Blocks
- Schutzlücke muss behandelt werden

Fragile Produkte

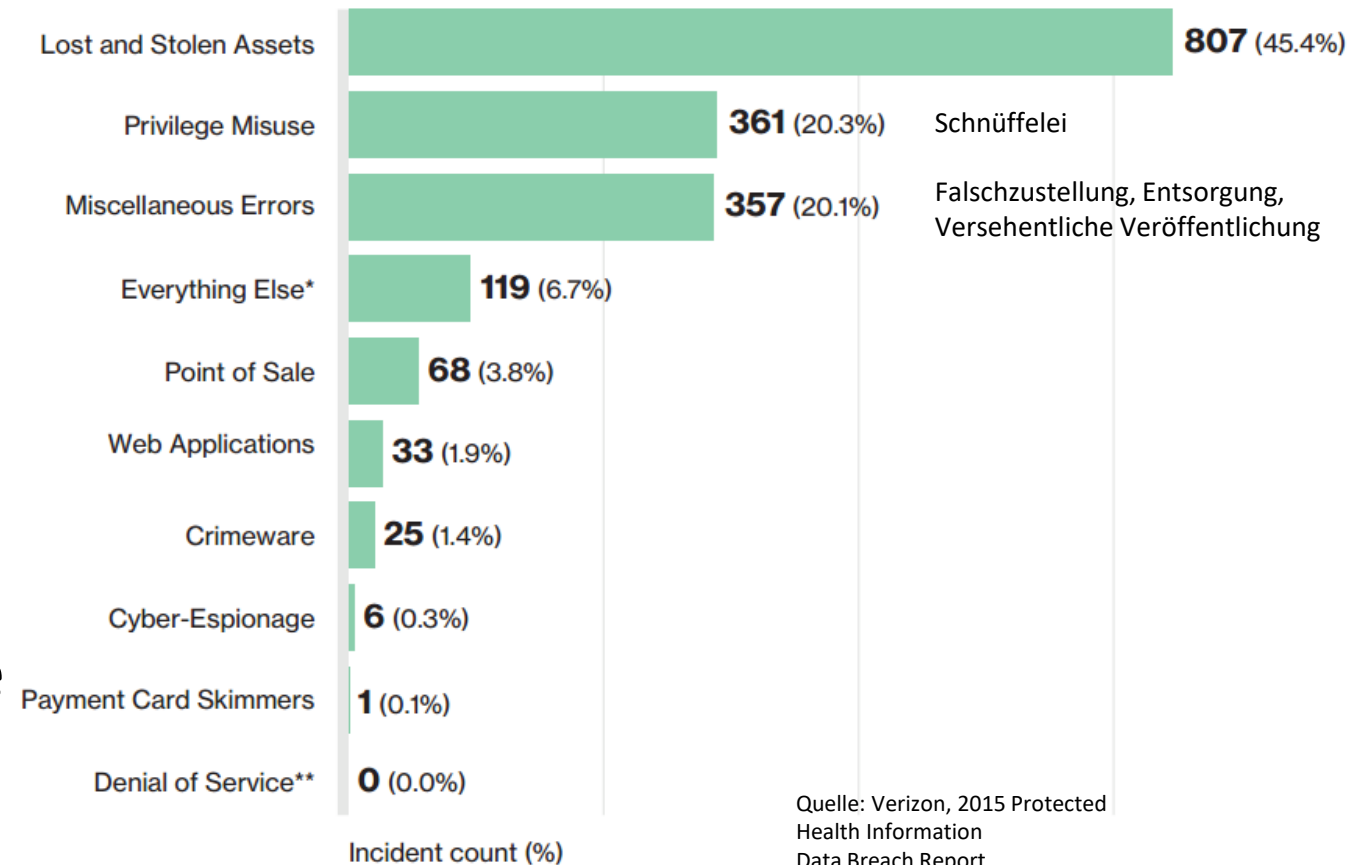
- Netzwerkfähige Geräte vertragen gelegentlich keine Daten
 - Patientenmonitoring
 - Drucker-Server
 - (unauthentisierter) Dateiserver für Diktiergeräte
- > Verfügbarkeit, Integrität

VERIS Community Database

- Öffentlich bekanntgewordene Sicherheitsvorfälle
- Maschinenlesbare Erfassung
- Bias: US-Gesundheitswesen, durch Veröffentlichung des U.S. Department of Health and Human Services (HHS)
- diverse Verizon-Berichte
 - Data Breach Investigations Report
 - Protected Health Information Data Breach Report

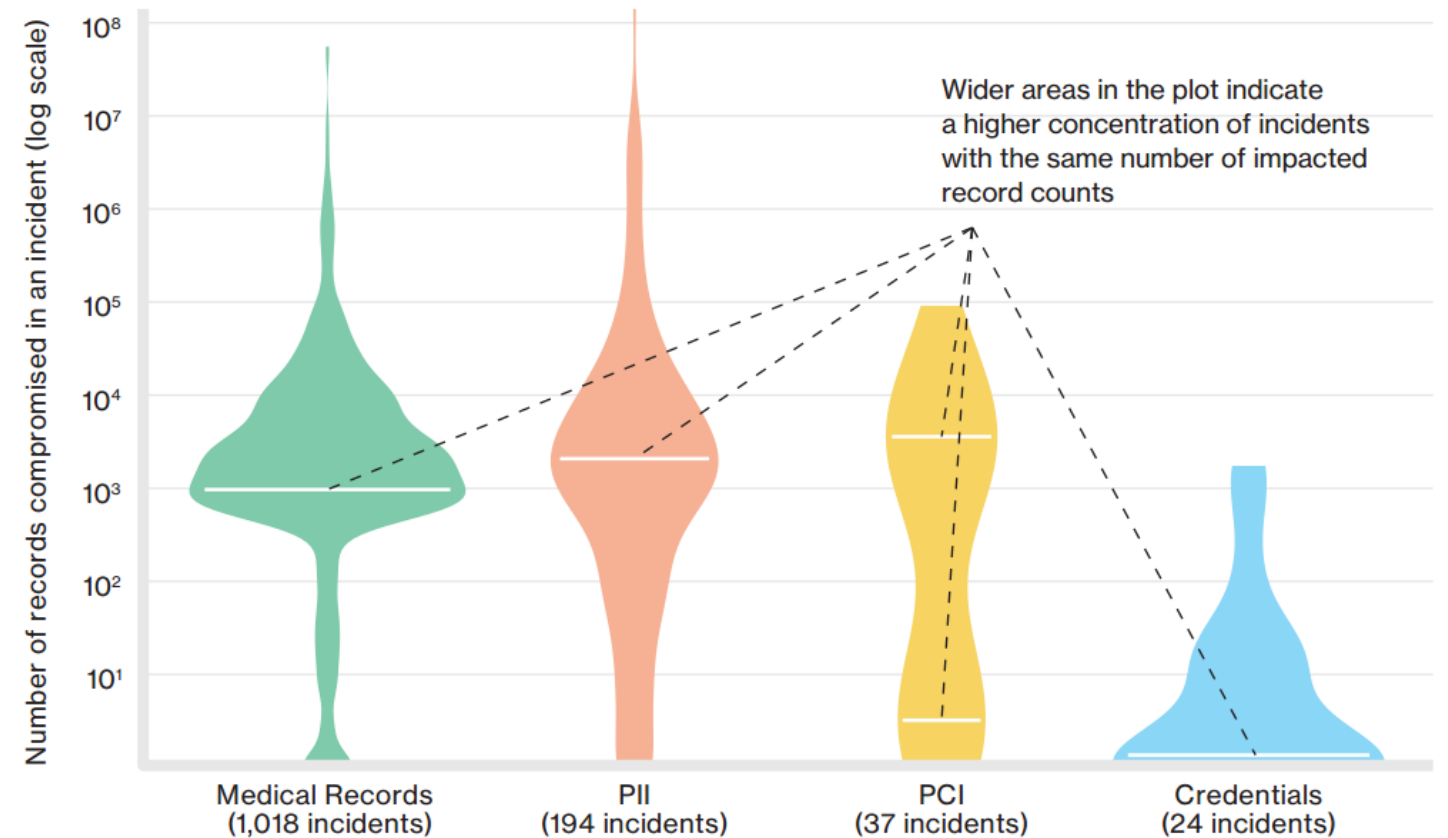
Protected Health Information Data Breach Report: “Nefarious Nine”-Muster

- 2015
- IT und analog
- 970 Vorfälle
- 25 Länder
- Knapp 300 Mio Datensätze enthüllt
- 3 Muster -> 85 % der Vorfälle
- 9 Muster -> 93 %



Protected Health Information Data Breach Report: Anzahl der betroffenen Datensätze

-> Risiko der Anreicherung



Quelle: Verizon, 2015 Protected Health Information Data Breach Report

Empfehlungen

- Einkauf:
 - Sicherheitsaspekte beim Einkauf verhandeln: Sicherheitsanforderungen, Security Development Lifecycle, Unterstützung bei Sicherheitsanalyse, sichere Integration, Incident-Handling, Kostenverteilung
- Integration:
 - Wenn Maßnahme nicht umsetzbar ist, müssen alternative/begleitende Maßnahmen umso besser sein
 - Lieber sicher im Alltag als nur auf dem Papier -> Testen (idealerweise inhouse)
- Betrieb:
 - Auf die Standardprobleme zuerst konzentrieren: “Nefarious Nine” und Standard-IT-Sicherheitsprobleme
 - Probleme zuerst adressieren, die keine Budgeterweiterung erfordern

Vielen Dank für Ihre
Aufmerksamkeit!

-

Diskussion

-

Kontakt:

Martin Schobert <martin@berlin.ccc.de>