Greenbone
Sustainable Resilience

Mit Greenbone eine nachhaltige Widerstandsfähigkeit erreichen

...wie Sie sich proaktiv gegen Cyberkriminalität schützen können

Heiko Melzow
Head of Sales
Greenbone Networks

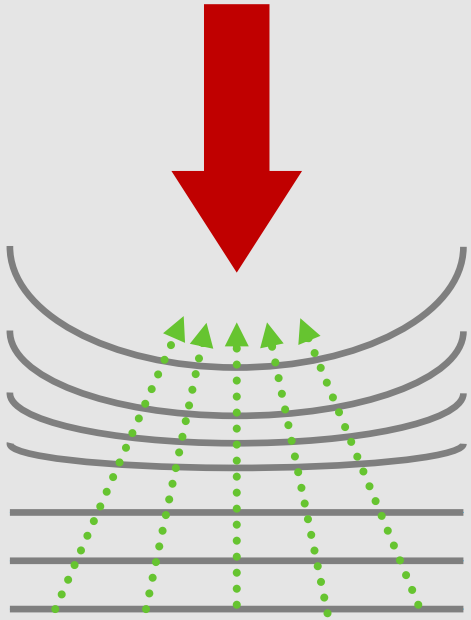
Über Greenbone und mich

- **Greenbone Networks GmbH**
  - Unabhängiger deutscher Hersteller
  - Der Greenbone Security Manager als Turn-key Appliance ist seit 2008 am Markt
  - Enstanden aus einer engen Kooperation mit dem BSI
  - Unsere Technologie wird in 30.000 Installationen weltweit verwendet
- **Heiko Melzow**
  - Partner Manager DACH
  - 20+ Jahre in der IT-Sec
  - Halte seit Jahren mehrere Herstellerzertifizierungen für Firewall & Security Vertrieb, u.a. für Palo Alto Networks, BlueCoat (Symantec), Fortinet,...

Charakteristik der Cyber Resilience

- Cyber Resilience entsteht, wenn IT Sicherheit tiefgreifend in die Unternehmensprozesse eingebunden ist. IT Sec kann nie absolute Sicherheit bieten, denn sie passt nicht zur modernen ‘networked interactivity’ eines Unternehmens. Resilience hat folgende Merkmale:

  - Priorisierung von Information Assets entsprechend des Business Risks.
  - Bereitstellen eines differenzierten Schutz für die wichtigsten Assets.
  - Integration der IT-Sicherheit in das unternehmensweite Risiko-Management und die Prozesse der Unternehmensführung und –kontrolle.
  - Beteiligung aller Mitarbeiter am Schutz der genutzten Information Asset.
  - Integration der IT-Sicherheit ins gesamte Technologie-Umfeld um CPS, OT, ICS, Scada.
  - Nutzen von ‘aktiven Verteidigungsmaßnahmen’, um die ‘Kosten’ für den Angreifer zu erhöhen.
  - Testen und kontinuierliches Verbessern der Security Posture in allen Geschäftseinheiten.



Greenbone
Sustainable Resilience

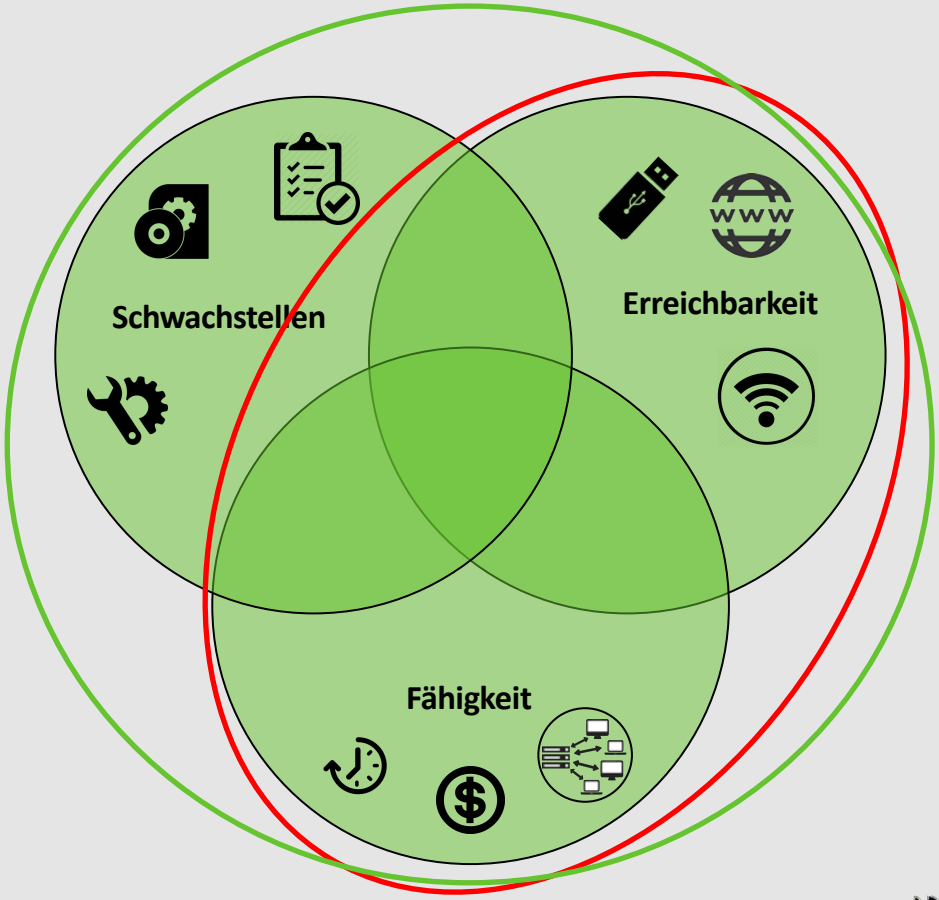
IT-Security versus Resilience (Widerstandsfähigkeit)

IT Sicherheit achtet meist nur auf die Bedrohung:

- Die Fähigkeit des Angreifers einen Angriff auszuführen
- Die Erreichbarkeit des Ziels, sowohl physisch oder virtuell (via Netz)

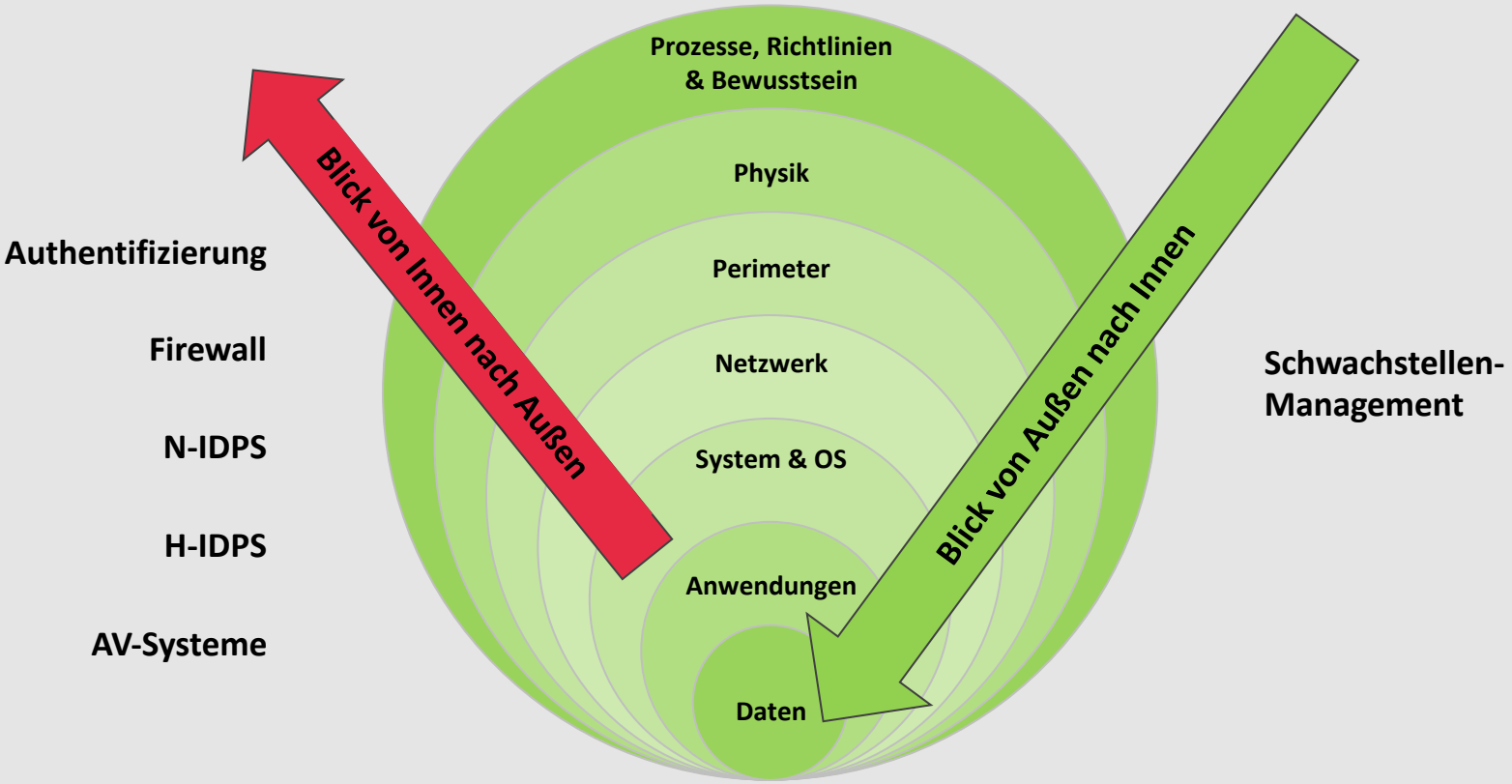
Resilience minimiert die eigenen Schwächen zur Stärkung der Basis:

- Software Fehler
- Basiskonfigurationen oder fehlerhafte Einstellungen
- Nicht-authorisierte oder unvermutete Installationen (Systeme, SW, Services, Shadow IT)
- Abweichung oder Nicht-Einhalten von Richtlinien, Vorgaben und Regeln.



Greenbone
Sustainable Resilience

Der Blickwinkel des Angreifers



Greenbone
Sustainable Resilience

ISO27001 & ISMS erwarten Vulnerability Management

- **Exec Summary in der ISO27001/2013**
  - In today's interconnected and mobile world, information is processed using systems and networks that employ state-of-the-art technology. It is vital to protect this information against both deliberate and accidental threats and vulnerabilities.

- **A.12.6: Technical vulnerability management**
  - Objective: To prevent exploitation of technical vulnerabilities.
  - A.12.6.1 – Control
    Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

- **ISO27002 und ISO27004**
  - ..02 Code of Practice – Implementation Guidance: „.. Systems at high risk should be addressed first .."
  - ..04 Monitoring, Measurement – Effectiveness measures:
    „.. the greater the number of known vulnerabilities and the longer that they are not addressed (e.g. patched), the greater the probability of their exploitation .."

VM vs. Pen Testing, Assessment oder Patch Management

- **Penetration Testing** ist ziel-orientiert; das Ziel ist die Übernahme der Kontrolle der IT-Infrastruktur. Ist das Ziel erreicht, wird nicht weiter nach der nächsten “offenen Tür” gesucht. VM sucht jede “offene Tür”.

- **Vulnerability Assessment** ist eine einmalige Evaluierung der IT-Infrastruktur, der jeweiligen “security posture”; Vulnerability Management ist der vollständige, kontinuierliche Prozess zur Steuerung, Regulierung und Verbesserung dieser Sicherheitslage.

- **Patch Management** ist ein wichtiger Baustein, doch was ist zuerst da: die Schwachstelle oder der Patch?

Widerstandsfähigkeit erhöhen, Angriffsfläche verkleinern

prepare

- Festlegen der Ziele zur eigenen IT-Sicherheit
- Was darf sein / was nicht
- Verknüpfen mit technischen Kontrollen

identify, classify, prioritize

- Welcher Fund muss zuerst bearbeitet werden
- Welcher hat die größte Wirkung

assign, mitigate & remediate

- Die richtige Person nimmt die notwendigen Veränderungen vor, hat dabei alle notwendigen Informationen zur Verfügung

store & repeat, improve

- Automatisierte, zeitgesteuerte Abläufe
- Darstellbare Verbesserung der IT-Sicherheit
- Erweiterung und Ergänzung der Zielsetzung

Greenbone
Sustainable Resilience

Greenbone
Sustainable Resilience

Ungeschützte Patientendaten im Internet
Eine weltweite Auswertung von Archivsystemen

Auszüge aus Greenbone‘s Sicherheitsbericht

Jan-Oliver Wagner
Geschäftsführer
Greenbone Networks

Unsere Sicherheits-Analyse: Ziel und Reichweite

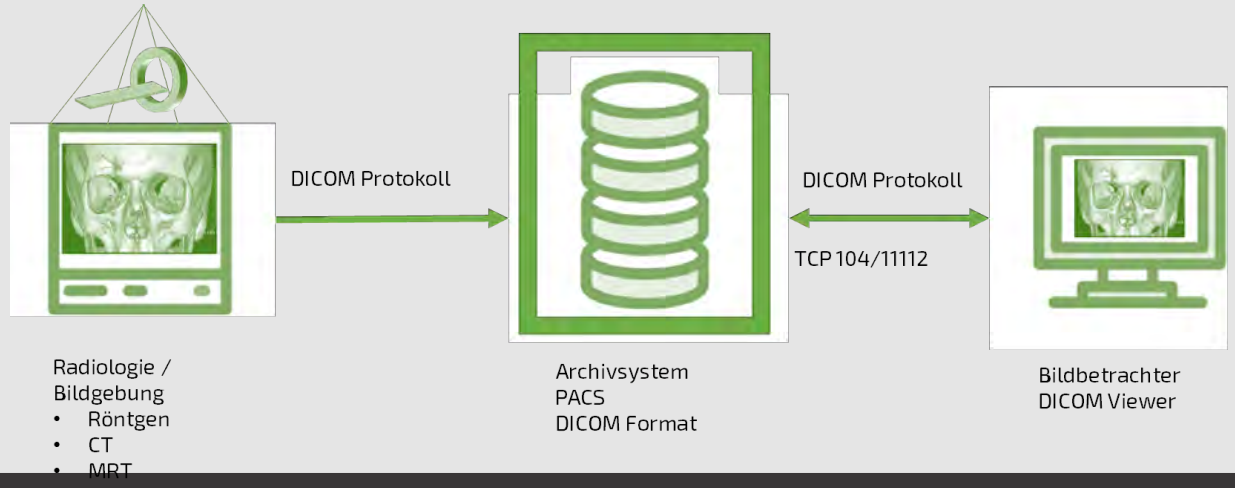
- Konkretes Ziel unserer Analyse waren sog. PACS Server, Archivierungssysteme für bildgebende Verfahren der Medizin,
  in denen **sensible Patientendaten** gespeichert werden.

- Identifiziert wurden **629** Systeme weltweit, die Zugriff auf Patientendaten erlauben, ohne Schutz, ohne Authentifizierung, unverschlüsselt. Betroffen sind Systeme in 52 Ländern der Welt. Als Grunddaten dienten IP-Adressen von ca. 2.300 Systemen
- Gefunden haben wir:

- **24,52 mio Datensätze**
- **738mio verlinkte Bilddaten**
- wovon wir auf **401mio Bilddaten Zugriff** hatten

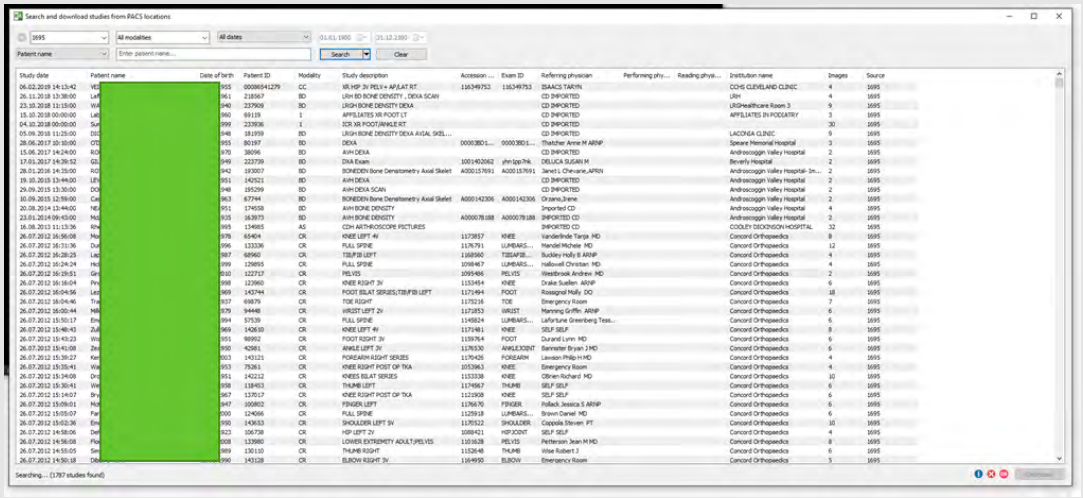
Kurzprofil des DICOM-Protokolls / -formats

- „DICOM (Digital Imaging and Communications in Medicine) is a standard for handling, storing, printing, and transmitting information in medical imaging. It includes a file format definition and a network communications protocol. The communication protocol is an application protocol that uses TCP/IP to communicate between systems. DICOM files can be exchanged between two entities that are capable of receiving image and patient data in DICOM format."

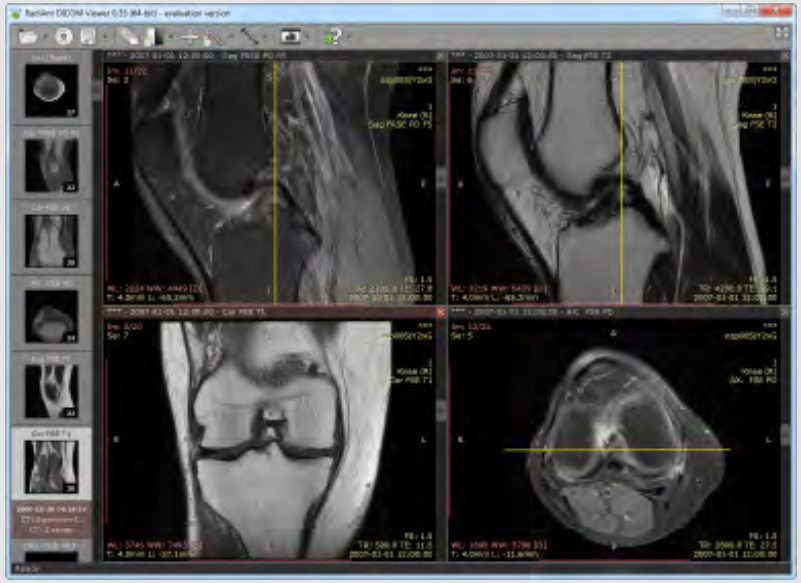


Kein Hack, nur Standardanwendungen

- Um auf die Daten zuzugreifen, wurde keine Software-Schwachstelle ausgenutzt, auch wurde kein Code, kein Script geschrieben.
- Um die Einfachheit des Zugriffs auf die Daten zu verdeutlichen, wurde eine Standard-Anwendung genutzt, ein sog. DICOM-Viewer.
  - Radiant DICOM Viewer



Originaldaten aus einen System



Beispiel, keine echten Bilder

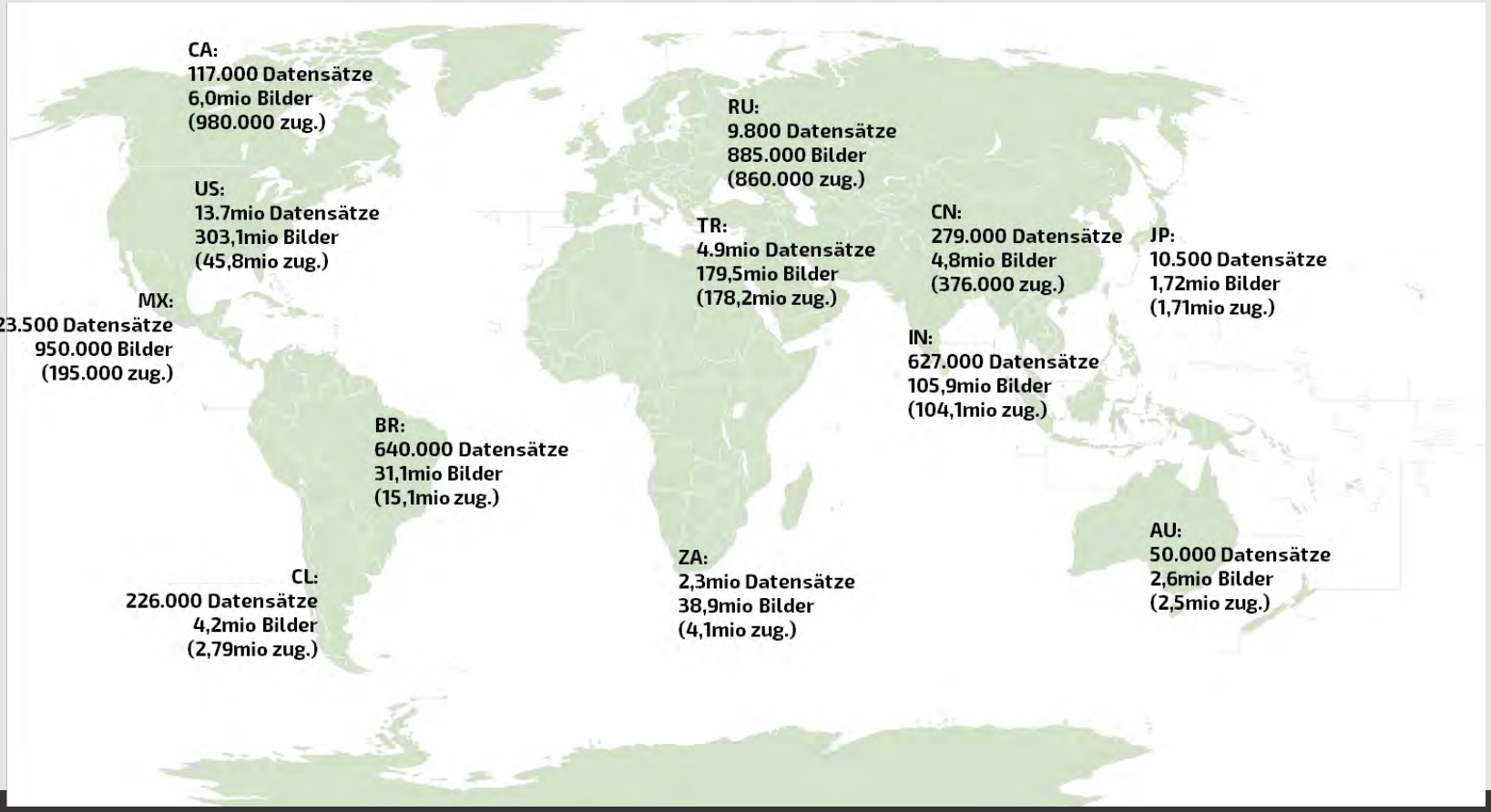
Europa

Für die Systeme in Deutschland sind die Daten und Abläufe wie folgt:

- 37 Systeme in Shodan/Censys gelistet
- davon 6 Systeme offen für Datenabfragen
- 15.000 Datensätze
- 2,85mio Bilder (davon 1,38mio abrufbar)
- Meldung ans BSI am 20.08
- Systeme in DE spätestens seit 13.09 nicht mehr erreichbar

- BSI hat andere Länder über die Funde vorort informiert.

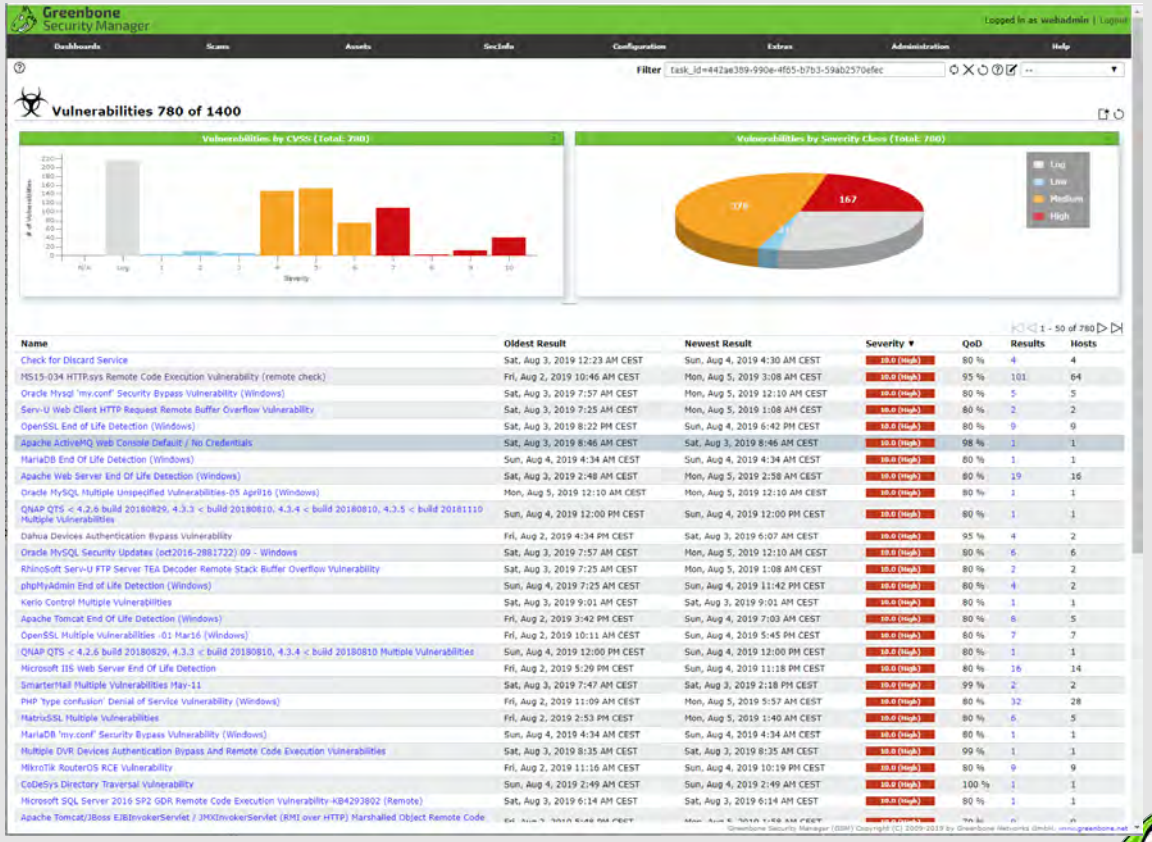
Wo die meisten Daten zu finden sind



Schlecht konfiguriert, nicht gewartet

Ein paar Fakten aus dem Report:

- Mehr als 10.000 Schwachstellen insgesamt (ohne Log-Meldungen)
- 2.000 als High, davon 500 als CVSS 10
- Häufung bei angreifbaren Webservern und Datenbank-Systemen
- IoCs enthalten



Was kann ein Angreifer damit machen?

- *„Medizinischer Identitätsdiebstahl“*
  Das Verwenden von medizinischen Daten einer anderen Person um eine medizinsche Dienstleistung zu erhalten, dazu zählen
  - Rezepte bzw. Ärztliche Verschreibungen
  - Operationen oder andere medizinische Behandlungen
  - Gefälschte Abrechnungen ggü. Krankenversicherungen
- *“Weaponizing” von Medizinischen Daten*
  Das Benutzen von sensiblen medizinischen Daten um einzelne Personen zu bedrohen, zu erpressen oder zu beeinflussen, um so:
  - Erpressungsgeld zu fordern
  - durch falsche oder echte zusätzliche Daten jemanden herabzuwürdigen
  - insbesondere Personen der öffentlichen Lebens sind gefährdet
    (Wir haben in unserem Research nicht nach Namen von VIPs in den Daten gesucht)
- *Geldbetrug*
  Ausnutzung der in den elektronischen Krankenakten enthaltenen persönlichen Daten (Personally Identifiable Information – PII) für die Erstelllung von Kreditkarten- oder Bank-Profilen um so einen Finanzbetrug zu ermöglichen.
  - Medizin-Dienstleister speichern oft Finanzinformationen zu Patientendaten
    (Wir haben Hinweise zu Abrechnungsinformationen in den Daten gesehen)
  - Kredite bzw Kreditlinien sind nicht selten an gesundheitliche Daten gekoppelt, die man in Patientenakten findet.
  - Steuerbetrug durch Abgabe falscher Abrechnungen
- *Cyber-Kampagnen*
  Medizinische Daten werden als ergänzende Daten in anderen, zukünftigen ‚Hacking Kampagnen‘ verwendet
  - Kontaktinformationen können für Phishing oder Scams (CEO Fraud, s.o.) benutzt werden
  - Credential/Authentication Informationen können für eine „privilege escalation“ genutzt werden.
    (Wir haben nicht nach solchen Informationen in den Daten gesucht)

Danke!
Ihre Fragen?

heiko.melzow@greenbone.net

Greenbone
Sustainable Resilience