HISOLUTIONS

Erlebnisse, Hürden und Herausforderungen eines KRITIS Prüfers

Hack im Pott 2020

Manuel (HonkHase) Atug

Über mich

Manuel Atug

Senior Manager der HiSolutions AG

> 23 Jahre in der Informationssicherheit tätig:

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen
- Spezialthemen: KRITIS, Hackback, Ethik, Bevölkerungsschutz

> 23 Jahre aktiv in so n paar Vereinen:

- Chaos Computer Club, Chaos Computer Club Cologne, c-base, Digitale Kultur, ISACA, GI, FIfF, Cyber Security Cluster Bonn, Freie Software Freunde, Gesellschaft für Freiheitsrechte, Geraffel Core Member
- Leitung der AG KRITIS: https://ag.kritis.info

AG KRITIS

Was ist KRITIS?

Regularien in Deutschland

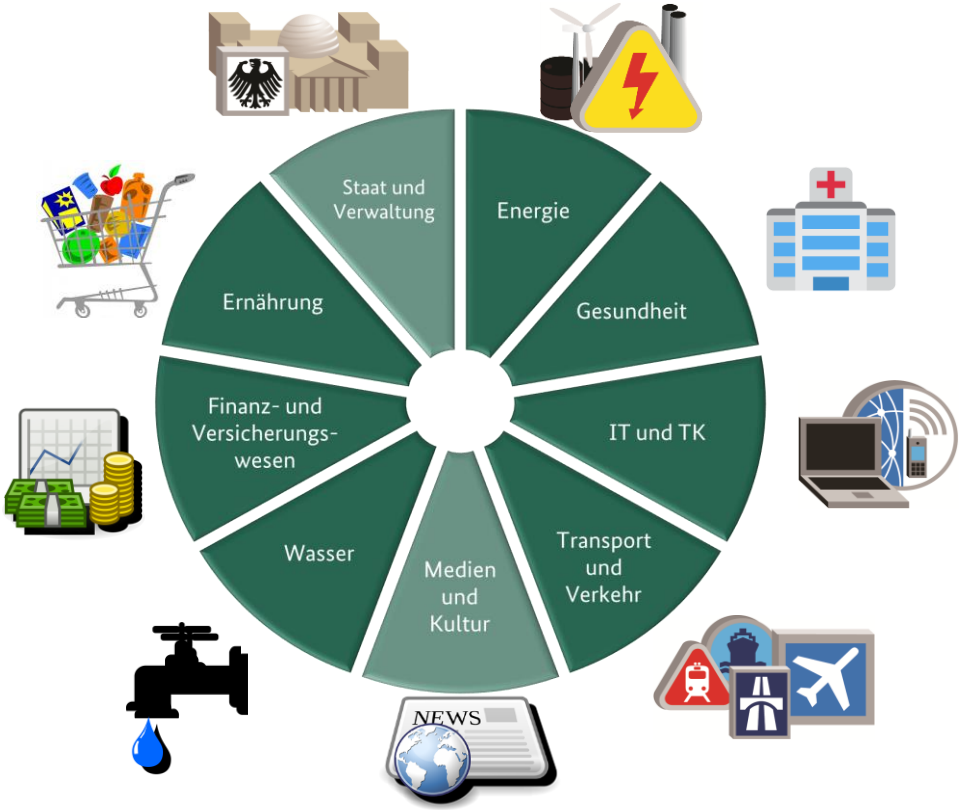
IT-SiG für kritische Infrastrukturen in 2015

Ziel: Sicherheit der IT-Komponenten von Kritischen Infrastrukturen

Rechtlich verbindlich ab einer Versorgung von 500.000 Bürgern

KRITIS Betreiber von neun Sektoren müssen ihre IT-Sicherheit nachweisen

Kritische Infrastrukturen



Quelle: BSI

KRITIS – Unterschiede zu anderen Sicherheitsstandards

- Dient dem Schutz der Bevölkerung (nicht des Betreibers)
- Es gibt KEINE Zertifikate!
- Dafür Ergebnisse: Mängelliste mit Sicherheitsmängeln
- Prüfkriterium: Umsetzung von Sicherheitsanforderungen (nicht die Planung)

Mangel ist nicht gleich Mangel

Man unterscheidend geringfügige Mängel und schwerwiegende Mängel

Keine Prüfung ohne Mangel?!

Das BSI fokussiert sich aktuell auf die schwerwiegenden Mängel

Die geringfügigen Mängel müssen aber auch behandelt werden ☺

Definition der Mängelkategorien

Schwerwiegender Mangel	• gravierende/erhebliche Gefährdung • akuter Handlungsbedarf
Geringfügiger Mangel	• Gefahr bzw. Risiko • kein akuter Handlungsbedarf
Empfehlung	• Verbesserungshinweis
Keine Abweichung	• Anforderungen vollständig erfüllt

Positiv hervorzuheben

Positiv hervorzuheben

Die **Verwendung eines B3S** erleichtert die Umsetzung bei KRITIS Betreibern enorm

IT-Sicherheit wird von vielen KRITIS Betreibern nun auch angegangen

Stärkere **Vernetzung der IT-Sicherheit** bei KRITIS Betreibern

KRITIS geht mehr und mehr in einen **Regelbetrieb** über

Das **BSI versteht** die Branchen immer mehr und führt **offene Gespräche**

Haben Sie mal ein Ersatzteil für uns?

Fehlende Ersatzteile

Industrie- und Produktionsanlagen laufen meist über einen sehr langen Zeitraum

Ältere Anlagen sind nicht auf Anforderungen zur Digitalisierung vorbereitet

Migrationsprojekte dauern viele Jahre

Kurios: Ersatzteile für geprüfte Anlage wurden in Kleinanzeigen gesucht, da Ersatzteile nicht mehr erhältlich sind

Bauliche Begebenheiten

IT-Systeme oft nachträglich eingebaut

RZ mitten unter der Hauptwasserleitung

Aktive Netzwerkkomponenten in ungelüfteten Abstellschränken

Safety vs. Security

Komponenten mit Safety Zulassungen

Neue Zertifizierung bei Anpassung von Komponenten erforderlich

Würdet ihr (außer ihr seid Prüfer) diese Komponenten gerne jeden Monat neu zertifizieren lassen?

Assetmanagement

IT ist oft (aber nicht immer) vorhanden

OT wird oft vergessen

Ohne Assetmanagement kein funktionales Riskolagebild oder BCM!

https://selinc.com/uploadedimages/Web/Videos/Playlists/PlaylistL_RTAC_1280x720.png?n=635847581260000

Physische Sicherheit

Pumpenhäuschen mit IT und GSM-Uplink

Generische Schließanlage aber keine Einbruchserkennung

Gimmick: WLAN und Bluetooth aber durchaus vorhanden

Beim Wort „Fernwartung“ leide ich innerlich immer ein bisschen!

Fernwartung

Fernwartung bzw. Fernadministration

Unzureichend gesicherte Remote Zugänge

Yet another Citrix #Shitrix...

Ferne Fernwartung

Unbekannte ferne Fernzugänge

z. B. auf Außenstationen oder Trafostationen

Unbekannt, aber vorhanden

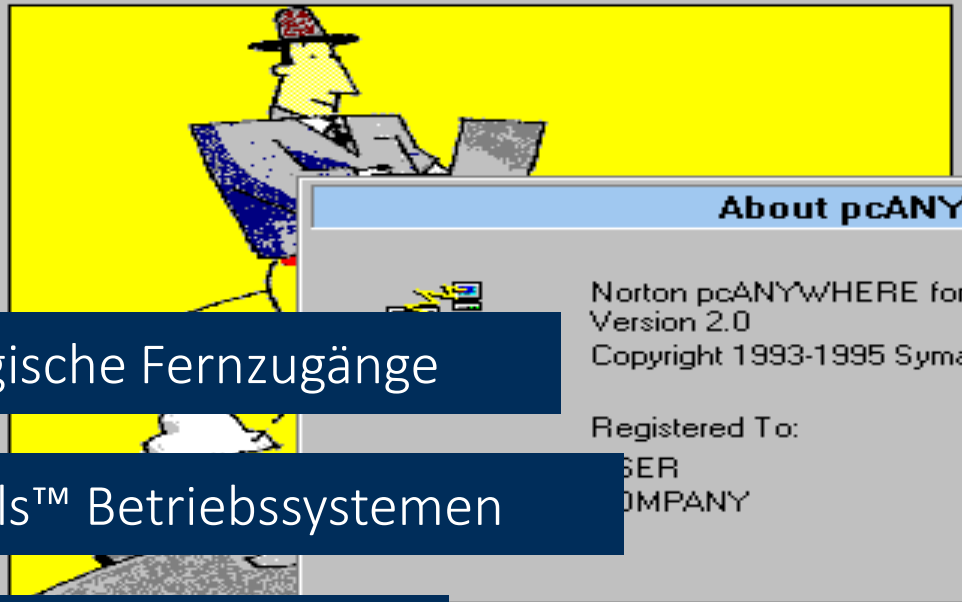
Ganz nahe ferne Fernwartung

Unbekannte ganz nahe Fernzugänge

z. B. Leitstand

Dienstleister hatte da mal eine Idee…

Fernwartungsarchäologie

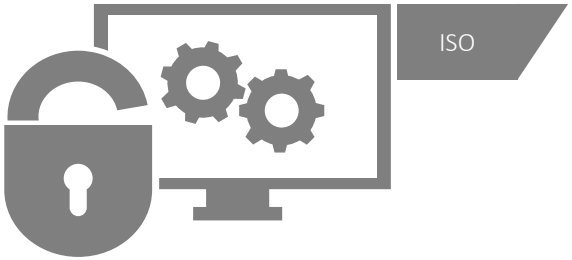


Archäologische Fernzugänge

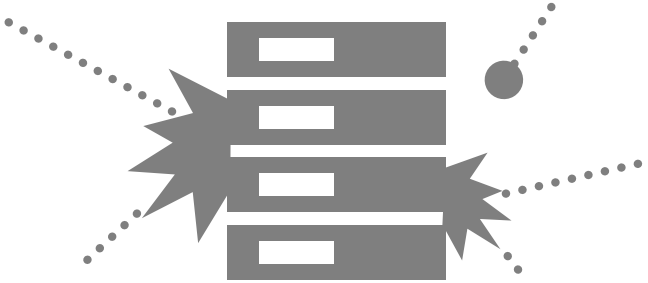
Auf damals™ Betriebssystemen

Install once, use forever

Typische Sicherheitsmängel bei Prüfungen



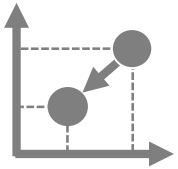
Umsetzung von ISO 27001
ohne Berücksichtigung von KRITIS



Reine Umsetzung technischer
Maßnahmen

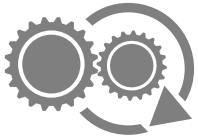
Typische Sicherheitsmängel bei Prüfungen

Branchentypische Gefährdungen nicht berücksichtigt



Risikomanagement rein aus Unternehmenssicht durchgeführt

Wichtige offene Maßnahmen nicht im Risikobehandlungsplan



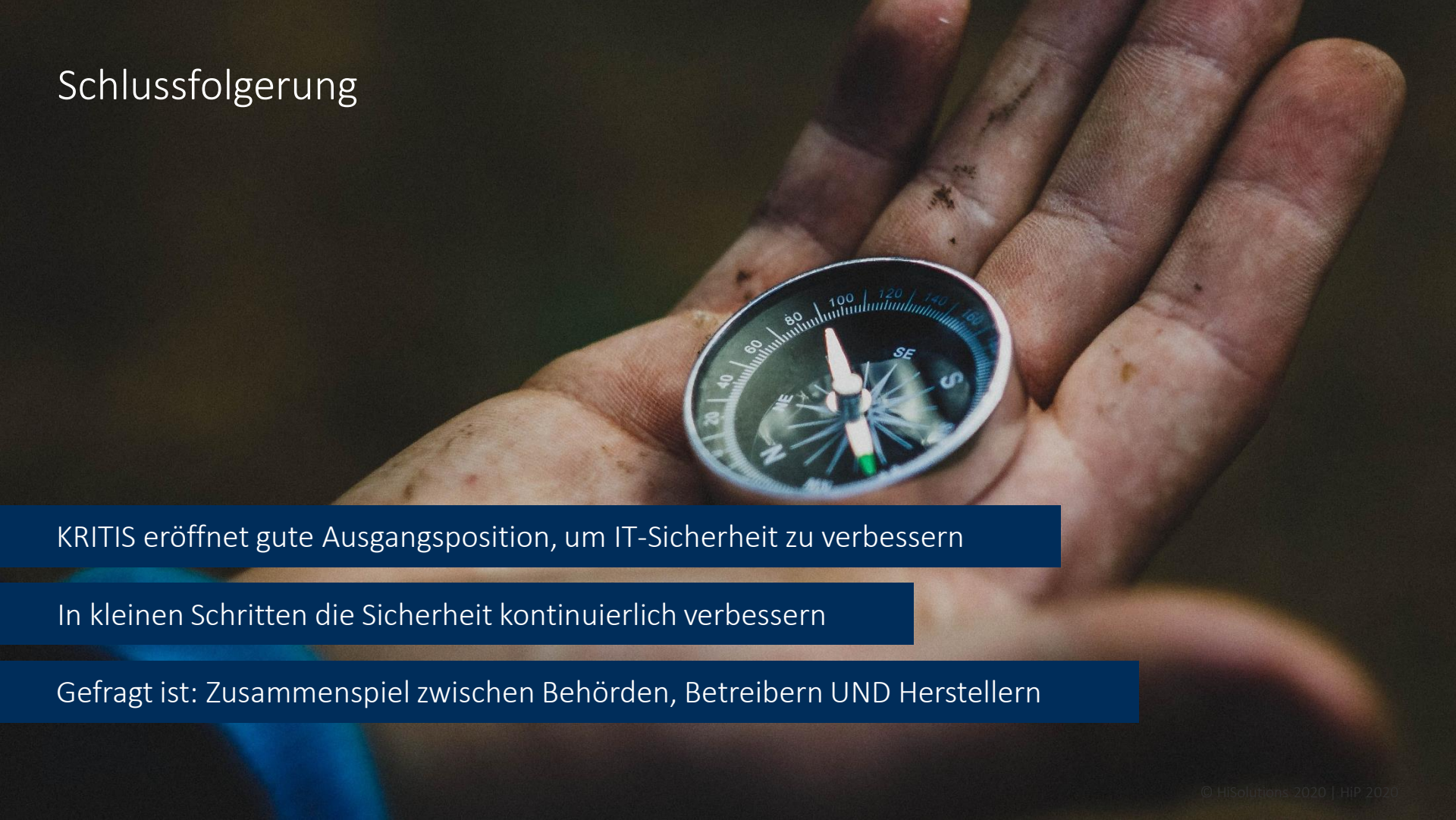
Business Continuity Maßnahmen nicht umgesetzt

KRITIS Umgebung zu klein gewählt

Asset Inventar nicht aktuell

Schlussfolgerungen

Schlussfolgerung



KRITIS eröffnet gute Ausgangsposition, um IT-Sicherheit zu verbessern

In kleinen Schritten die Sicherheit kontinuierlich verbessern

Gefragt ist: Zusammenspiel zwischen Behörden, Betreibern UND Herstellern

Abgrenzung zu KRITIS nach § 8a BSIG

KRITIS deckt nur den IT-gestützten Teil der kritischen Infrastrukturen ab!

Was fällt nicht darunter:

- Umwelteinflüsse
- Probleme in der Supply Chain durch Verkehrsprobleme
- Zu warmes Kühlwasser aus Flüssen
- Streik
- Virus-Pandemie

Bouchéstraße 12 | 12435 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com