# Cyber-Kriminalität: Gefahren (er)kennen, den Spagat zwischen Wunschdenken und Ist-Zustand meistern und sich wirksam schützen

**Europäischer Verwaltungskongress 2022 in Bremen**

Kom-CERT, regio iT, Thomas Stasch

regio iT

# Vorstellung

## Persönliches

- 50 Jahre alt
- verheiratet
- zwei Kinder
- Diplom Informatiker (FH)
- Master of Science Wirtschaftsinformatik

## Lebenslauf

- Mitarbeiter Stadtkasse bei der Kreisstadt Siegburg, 1991
- Systemadministrator bei der Kreisstadt Siegburg, bis 1999
- Service Manager bei der Deutschen Post DHL, IT-Services GmbH, bis 2010
- Leiter Stabsstelle IT-Sicherheit und Service Management bei civitec
- Leiter civitec-CERT beim Zweckverband civitec
- Leiter KomCERT und Informationssicherheitsbeauftragter bei der regio iT GmbH

- Nebenberuflich: Dozent für IT-Security, Wilhelm Büchner Hochschule

# Ist Ihre Kommune schon smart?
# Ist Ihr Zuhause schon vernetzt?

## Nutzen Sie das IoT – Internet of Things - Das Internet der Dinge!

#allwayson #musthave #smart

- **Apples Smart-Watch**
  EKG-Funktionen, Mailing und auch noch die Uhrzeit
- **Die Smarte Windel**
  Die smarte Windel Opro9 misst Feuchtigkeit und Temperatur und gibt über eine App auf dem Smartphone.
- **Smarte Cities**
  Informieren über freie Parkräume, melden Falschparker, zeigen Verkehrsflüsse.
- **…**

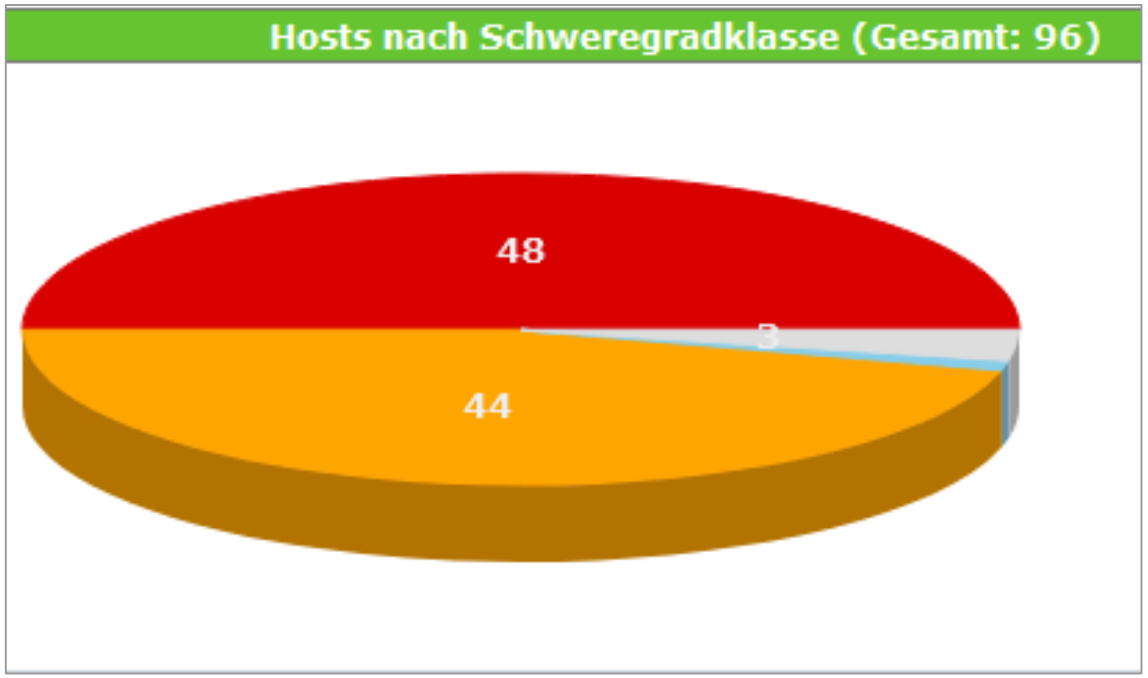
# Nicht nachmachen!!!

# Auswirkung von Schwachstellen (log4j)




**log4j:**
Ein **entfernter**, **anonymer** Angreifer kann eine Schwachstelle in Apache log4j ausnutzen, um **beliebigen Programmcode auszuführen**.

## Schwachstellenscan einer Kommune

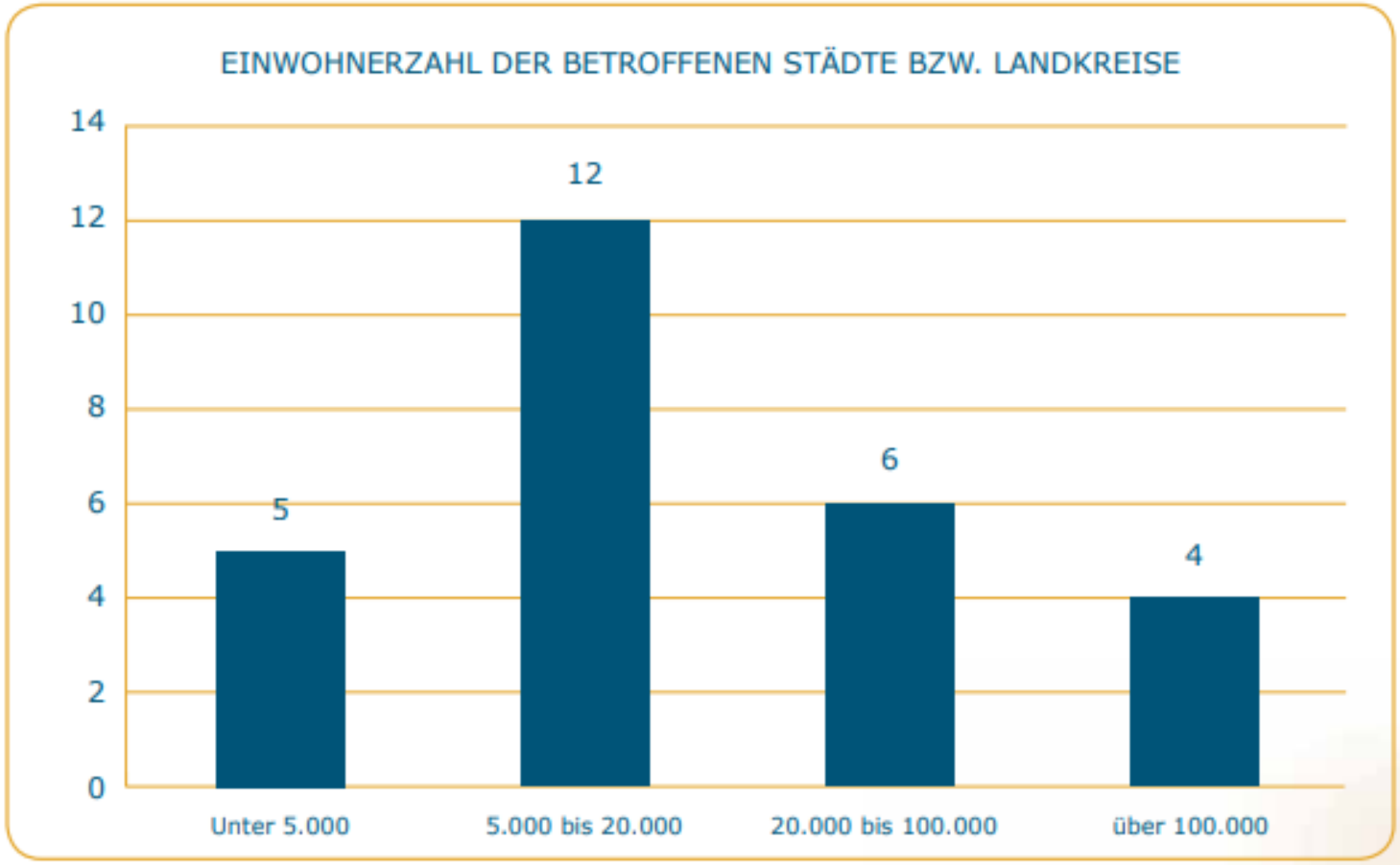



**Die kommunale Praxis zeigt leider noch deutliches Potenzial in Sachen Patch-Management und somit große Angriffsflächen für Cyber-Angriffe.**

# Die kommunale Wirklichkeit

# Untersuchung von 27 Cyberangriffen auf deutsche Kommunen in 2021

Abbildung 1: Einwohnerzahl der betroffenen Städte bzw. Landkreise




Quelle: Darstellung aus Studie von Esther Kern (2022) „Cyberangriffe auf deutsche Kommunen im Jahr 2021“, BIGS Essenz Nummer 19.

## Aktuelle Vorfälle

- Stadt Witten
- Autovermietung Hertz
- Aviation Services AHS
- Stadt Suhl
- Polizei Hessen
- Krankenhaus Braunschweig
- Stadtwerke Pirma
- Stadtverwaltung Ebeleben
- Landmaschinenhersteller Fendt
- DDoS Angriffe gegen Behörden
- …


Angeblich 20 Terabyte abgezogen: Hackerangriff auf deutsche Tochter von Rosneft

Die deutsche Niederlassung des größten russischen Ölproduzenten ist Ziel eines Cyberangriffs geworden. Dabei wurde angeblich einiges an Schaden angerichtet.


CYBERKRIMINALITÄT

Nach Hackerangriff: Stadt Suhl nach wie vor lahmgelegt

von MDR
Stand: 14. März 2022, 15:44 Uhr

TEILEN VIA Facebook Twitter Pinterest Email

Die Stadtverwaltung in Suhl ist in Folge des **Hackerangriffs** immer noch weitestgehend arbeitsunfähig. Wie ein Sprecher MDR THÜRINGEN sagte, konnte der Zugriff auf die digitalen Daten und Systeme bisher nicht wiederhergestellt werden. Es werde daran gearbeitet, die Systeme wieder einsatzfähig zu machen. Priotität habe das Gesundheitsamt.


Angehefteter Tweet

**Anonymous** @YourAnonOne · 24. Feb.

The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine

9.107 60.603 316.218


FOCUS-Reporter **Josef Hufelschulte**

Freitag, 18.03.2022, 12:34

**Der russische Militärgeheimdienst GRU soll nach einem Bericht des Nachrichtenmagazins FOCUS potenzielle Angriffsziele in Deutschland ausspioniert haben.**

Das Bundesamt für Verfassungsschutz untersucht derzeit ernstzunehmende Hinweise auf Objekte in **Berlin** und Sachsen, die im Kriegsfall von Spezialkräften der **russischen** Armee attackiert werden könnten. Bei diesen Zielen soll es sich unter anderem um Einrichtungen

## Teppich… da kann man einiges drunter kehren ☺

# „Nie passiert“ – Aus dem Leben eines kommunalen CERTs 1/2

Kommunen neigen dazu „bitte keine Informationen nach außen“ zu geben.
So sind folgende Fälle des KomCERT „völlig hyperthetisch“

**Verschlüsselung eines kompletten Berufskollegs**

- File-Server
- Mail-Server
- Datensicherung

- 25.000 EUR Lösegeld-Forderung

# „Nie passiert“ – Aus dem Leben eines kommunalen CERTs 1/2

Geschäftsführer
kommunales Unternehmen

Kaufmännischer Leiter
kommunales Unternehmen

Hallo Herr XXX,
Sind Sie gerade Verfügbar?
Mit freundlichen Grüßen,
**YYY - Geschäftsführer**

Hallo Herr YYY,
ich bin in einigen Terminen. Was gibt es denn? Etwas Dringendes?
Beste Grüße
**XXX – Kaufmännischer Leiter**

Ich brauche Ihre Hilfe in Bezug auf die vertraulichen Finanztransaktion . Können Sie mit Priorität arbeiten?
(dass unsere Gespräche ausschließlich über E-Mail)
Mit freundlichen Grüßen,
**YYY - Geschäftsführer**

Hallo Herr YYY,
wenn Sie sagen mit Priorität, werde ich es irgendwie möglich machen.
Sie wissen aber, dass ich jetzt gleich zur Finanztagung muss und erst morgen früh wieder im Office bin, oder?
Um was geht es denn?
Schöne Grüße
**XXX – Kaufmännischer Leiter**

…

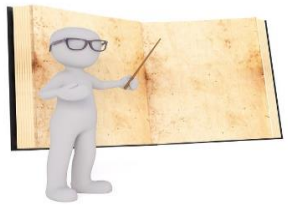
# Investitionen in die Sicherheit

**Know-how**
Ausbildung von Security Fachkräften – Sensibiiisierung der Mitarbeitenden und Kunden

**Kooperation**
Zusammenarbeit auf nationaler Ebene zwischen den Sicherheitsteams

**Reaktionsfähigkeit**
Konsolidierung und Stärkung des Business Continuity Managements  für den Krisenfall

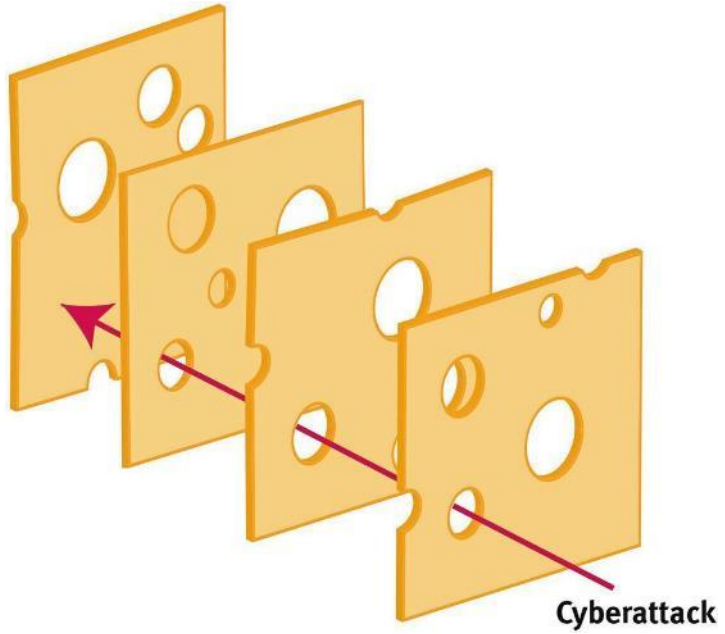
**Ausbau der Detektionsmöglichkeiten**
Angriffe und Versuche frühzeitig erkennen und agieren.



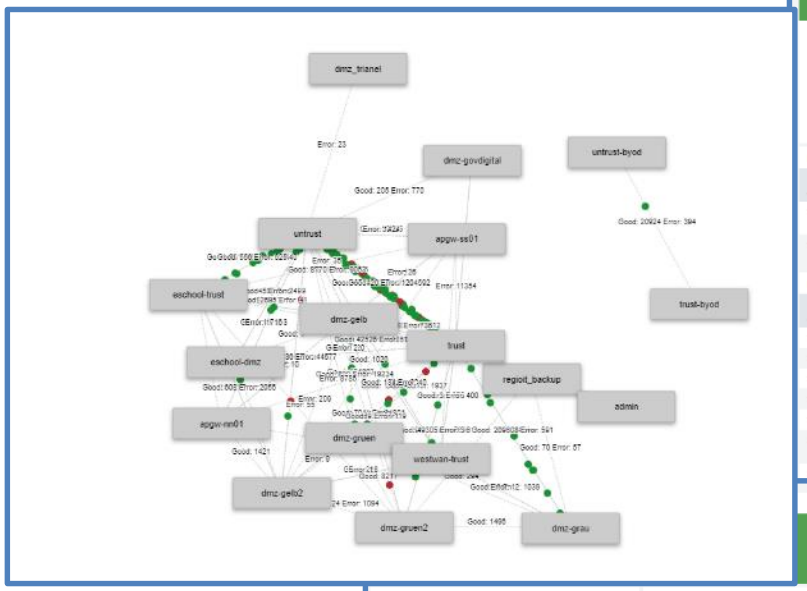
**Technologie**
Nutzung neuer technischer Ansätze in der Cyber-Defense: Von Backup über Virenschutz bis zu künstlichen Intelligenz

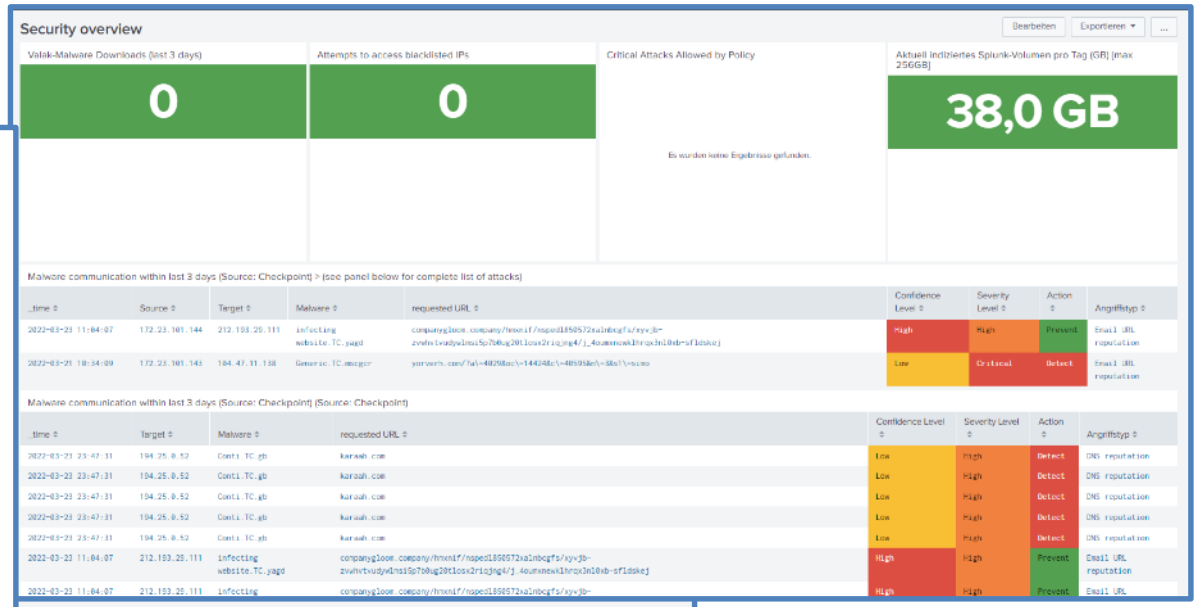
**Nur im optimalen Zusammenspiel von Systemen und Menschen kann es gelingen, die Eintrittswahrscheinlichkeit zu reduzieren.**

**Der beste Schutz sitzt immer noch 60 cm vor dem Bildschirm ➔ aktivieren Sie ihn!**



# Security Monitoring (SIEM) – teuer aber sinnvoll - SOC




## Kommunales Grundschutzprofil

Dieses IT-Grundschutz-Profil richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen. Es ist adressiert an die Verantwortlichen in der Verwaltung, welche für die Umsetzung und Aufrechterhaltung der Informationssicherheit zuständig sind. Dies sind typischerweise die Hauptverwaltungsbeamtinnen und -beamten, welche die Ressourcen bereitstellen und das angestrebte Sicherheitsniveau einschließlich der Risiken verantworten, sowie die für die Steuerung und Koordination des Informationssicherheitsprozesses zuständigen Informationssicherheitsbeauftragten.

Dieses Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, um sich nach hiesiger Einschätzung nicht der groben Fahrlässigkeit schuldig zu machen.

### 9.1.4 ORP.3 - Sensibilisierung und Schulung zur Informationssicherheit

| **Anforderungen** | **ORP.3.A1 – A3; A6** |
|---|---|
| **Besonderheiten** | ORP.3.A6<br>Um sicherzustellen, dass Sicherheitsmaßnahmen nicht versehentlich falsch umgesetzt oder unwissentlich ignoriert werden, müssen Mitarbeiter strukturiert und fortlaufend sensibilisiert werden. |

# Vielen Dank für Ihre Aufmerksamkeit!

www.regioit.de
Thomas Stasch, komcert@regioit.de

regio IT