ekom21

Die Zukunft der Verwaltung


# Kommunale Informationssicherheit in Hessen

# Kurzvorstellung ekom21 KGRZ Hessen - Historie

- 1970 – Gründung von fünf kommunalen Gebietsrechenzentren (DA/WI/F/GI/KS)
- 1996 – Zusammenschluss von drei KGRZ (DA/F/GI) zur KIV (Kommunale Informationsverarbeitung) Hessen
- 2001 – Gründung der ekom21 GmbH (100%-ige Tochter)
- 2008 – Zusammenschluss KIV Hessen und KGRZ Kassel zur ekom21 – KGRZ Hessen mit Geschäftssitz in Gießen

# Kurzvorstellung - Unternehmen

**ekom21** steht für das **größte** BSI-zertifizierte kommunale IT-Dienstleistungsunternehmen in Hessen, für das **drittgrößte** in Deutschland.

# Allianz gegen Cyberkriminalität

KDLZCS

KOMMUNALES
DIENSTLEISTUNGSZENTRUM
CYBERSICHERHEIT
HESSEN

# Allianz gegen Cyberkriminalität

Die ekom21-KGRZ Hessen hat am 28. Januar 2016 zusammen mit dem hessischen Innenminister Peter Beuth und den Vertretern der kommunalen Spitzenverbände eine gemeinsame Sicherheitsinitiative vorgestellt:

Das Kommunale Dienstleistungszentrum Cybersicherheit Hessen (**KDLZ CS**).

Im Fokus stehen zunächst Städte und Gemeinden bis ca. 30.000 Einwohner, weil diese in der Regel keine eigenständigen IT-Abteilungen mit entsprechend ausgebildeten Spezialisten vorhalten.

# Allianz gegen Cyberkriminalität

Rahmenbedingungen :

- **Finanzielle Förderung** zum Aufbau des **K**ommunalen **D**ienst**l**eistungs**z**entrums **C**yber**s**icherheit durch das **Land Hessen**

- **Vorbereitung** auf zukünftige gesetzliche Vorgaben zu Maßnahmen im Bereich IT-Sicherheit

# Projektziel

- **Gemeinsame** Sicherheitsoffensive des **Landes Hessen**, der **Kommunen** und der **ekom21** zur Erhöhung der Informationssicherheit in hessischen Städten und Kommunen.

- Schaffung einer möglichst großflächigen **Verbesserung des Informationssicherheitsniveaus** bei den Städten und Kommunen

# Projektstatistik – Stand 18.04.2016

- Offizieller Projektstart: 28.01.2016 in Idstein

- Anzahl interessierter Kommunen: 68
- Anzahl bestätigter Termine: 47
- Anzahl Vorgespräche: 11
- Anzahl der Termine „Bestandsaufnahme“: 36
- Anzahl qualifizierter Berater: 12

# Reale Bedrohung aus der virtuellen Welt

## Rodgau schließt Datenleck

30/10/2014

### Stadtverordnete sorgen sich dennoch um Sicherheit

cbor. RODGAU. Die Stadt Rodgau hat nach eigenen Angaben eine Sicherheitslücke im Computernetz der Verwaltung geschlossen, durch die personenbezogene Daten eingesehen werden konnten. Damit reagierte sie auf einen Hinweis der Stadtverordnetenfraktion „Zusammen mit Bürgern“ (ZmB).

Im Juni hatten Stadtverordnete der ZmB entdeckt, dass sie im internen Netz der Verwaltung auf einen Ordner zugreifen konnten, der unter anderem Informationen zu Gehaltsüberweisungen und Kontodaten der städtischen Bediensteten sowie zu Strafangelegenheiten enthielt. Nach Darstellung der ZmB-Fraktion unternahm die Stadt sieben Wochen lang nichts, obwohl man am Tag der Entdeckung umgehend den Bürgermeister und den Ersten Stadtrat informiert habe.

Eine Sprecherin der Stadt sagte, man habe sofort auf die Information reagiert und den Inhalt des Ordners gelöscht. Da man den Ordner selbst aber stehen gelassen habe, könne der Eindruck entstanden sein, die Daten seien noch verfügbar. Es könne sich auch um zwischengespeicherte Daten gehandelt haben. Die ZmB spricht allerdings davon, dass aktualisierte Daten sichtbar gewesen seien.

Ursache für das Datenleck war nach Angaben der Stadt eine falsche Vergabe von Zugriffsrechten in der Software. Eine externe Firma habe das Netzwerk untersucht und den Fehler behoben. Dabei seien auch einige kleinere Probleme sichtbar geworden, die ebenfalls beseitigt worden seien.

Die ZmB-Fraktion hat den Vorfall zum Anlass genommen, den Magistrat um eine Stellungnahme zum Datenschutz zu bitten. Bis Ende November soll er sich unter anderem dazu äußern, ob es in den vergangenen drei Jahren Fälle von Datenmissbrauch gegeben habe, was dagegen unternommen worden sei und welche Mitarbeiterschulungen zum Thema abgehalten worden oder geplant seien.

## Hacker verursachten Stromausfall

FAZ 10/1/16

### Erkenntnisse über einen Cyberangriff in der Ukraine

Bei einem Stromausfall, der am 23. Dezember im Westen der Ukraine 700 000 Haushalte betraf, handelt es sich wahrscheinlich um eine Sabotage über das Internet. Wie Firmen für Internetsicherheit, darunter das slowakische Unternehmen Eset, berichteten, fanden sich auf den Computern eines ukrainischen Stromversorgers Kopien der Schadsoftware „Black Energy“. Offenbar waren Mitarbeiter des Versorgers durch eine E-Mail mit gefälschtem Absender dazu gebracht worden, ein Programm zu starten, das „Black Energy“ installierte, wodurch die Hacker Zugang zu dem System bekamen. Auf welche Weise sie dann den Stromausfall herbeiführten, ist allerdings nicht geklärt, da es ihnen gelang, viele ihrer Programmmodule anschließend wieder zu löschen. Auch die Herkunft der Saboteure konnte daher bislang nicht ermittelt werden.

Der Angriff wäre die bisher dritte Cyberattacke, die physische Schäden an großtechnischen Anlagen verursacht hat. Zuvor war 2010 der Computerwurm „Stuxnet“ entdeckt worden, der iranische Nuklearanlagen beschädigt hatte. Im Jahr 2014 beschrieb ein Bericht des Bundesamtes für Sicherheit in der Informationstechnik einen erfolgreichen Angriff auf ein deutsches Stahlwerk. *Wissenschaft*

# Reale Bedrohung aus der virtuellen Welt

FRANKFURTER ALLGEMEINE ZEITUNG

## Digitaler Angriff auf die Gesellschaft

Die Attacken von Hackern erreichen neue Dimensionen. Nach Unternehmen nehmen sie nun auch staatliche Stellen ins Visier. Die Gefahren sind riesig, die Schäden noch nicht auszumachen. Das politische Berlin ist alarmiert – und die Unsicherheit wächst messbar.

fib./tih. FRANKFURT, 23. Juni. Die Attacken auf Computer und digitale Netzwerke haben eine neue Dimension erreicht. Nachdem in Amerika, Asien und Mitteleuropa viele Unternehmen, Verwaltungen und Behörden betroffen waren, sind nun auch staatliche Einrichtungen in Deutschland ins Visier der Angreifer geraten. Dabei nehmen die Angreifer vor allem die Verkehrsinfrastrukturen zwischen Kimme und Korn. Die digitalen Heckenschützen sind noch nicht ausgemacht, die Schäden nicht beziffert, doch die Gefahren sind riesig.

Kurz nacheinander haben Hacker in den vergangenen Tagen und Wochen da-

Datenpanne in Wiesbaden

## Hacker beantragen erfolgreich Briefwahlunterlagen für OB

Veröffentlicht am 25.01.16 um 21:37 Uhr

**Jede Wähleradresse wäre so abrufbar gewesen**

# Reale Bedrohung aus der virtuellen Welt

**Tesla-Crypt: Erpressung mit Trojaner - Stadtverwaltung zahlte Lösegeld**

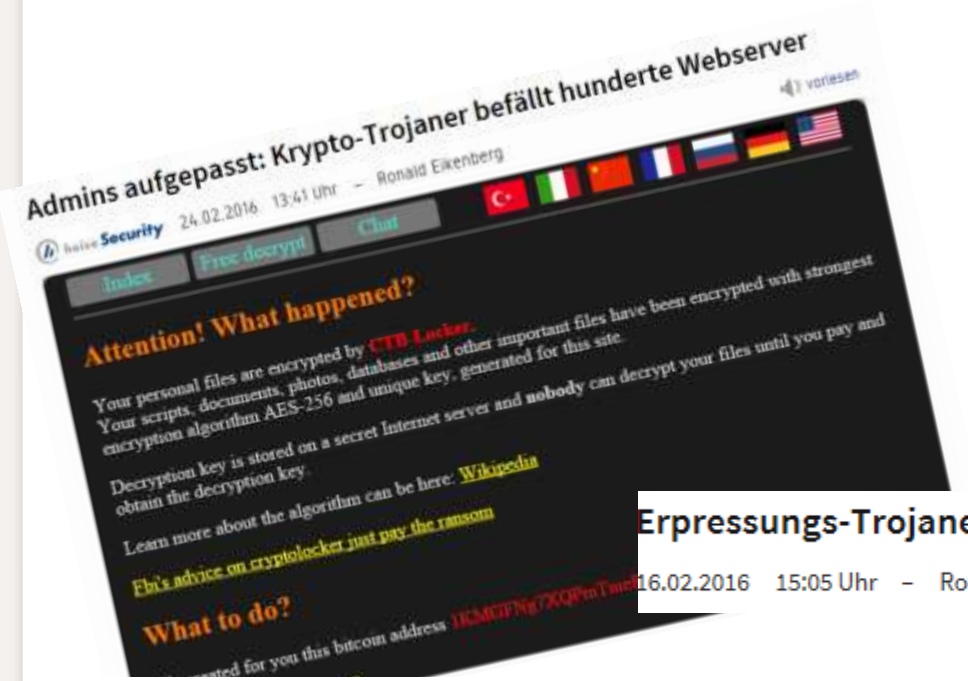
*Von Jörg Diehl und Björn Hengst*

**Ein Erpressungs-Trojaner hatte die Stadtverwaltung im unterfränkischen Dettelbach weitgehend lahmgelegt. Die Behörde sah sich gezwungen, das verlangte Lösegeld zu zahlen.**

Teilen Twittern E-Mail +

Donnerstag, 03.03.2016 – 17:42 Uhr

# Reale Bedrohung aus der virtuellen Welt





**Erpressungs-Trojaner Locky schlägt offenbar koordiniert zu** UPDATE

16.02.2016 15:05 Uhr – Ronald Eikenberg vorlesen

**Ransomware: Neben deutschen Krankenhäusern auch US-Klinik von Virus lahmgelegt**

16.02.2016 10:48 Uhr – Martin Holland vorlesen

**Krypto-Trojaner Locky wütet in Deutschland: Uber 5000 Infektionen pro Stunde**

19.02.2016 06:15 Uhr – Ronald Eikenberg vorlesen

# Vorgehensmodell


- Bestandsaufnahme eines Mitarbeiters des KDLZ-Cybersicherheit mit standardisiertem Fragebogen
- Besprechung der Ergebnisse und den sich daraus ergeben-den notwendigen Maßnahmen
- E-Learning der Mitarbeiter
- Präsenzschulung der Mitarbeiter
- Bereitstellung von Erläuterungen und Vorlagen zur Etablierung eines ISMS
- Kontrolle auf Umsetzung der notwendigen Maßnahmen

# IT-Sicherheitsleitlinie

Das Grundgerüst einer nachhaltigen Sicherheitsstrategie ist die **Einführung** sowie in der Folge die **regelmäßige Aktualisierung** einer IT-Sicherheitsleitlinie.

Diese verdeutlicht einerseits, welchen Stellenwert die Informationssicherheit in der Kommune hat und regelt andererseits die Verantwortlichkeiten.

Diese **Verbindlichkeit** bildet eine Handlungsgrundlage aller Mitarbeiter rund um die **Informationssicherheit**.

**Vielen Dank für Ihre Aufmerksamkeit!**