Kommunale Versorgungskassen Westfalen-Lippe

„Cyber-Ritter: Eine epische Reise durch die IT-Sicherheit“

Nicklas Baier, IT-Sicherheitsbeauftragter

// Auf dem Schlachtfeld der Cybersicherheit: Ein brisanter Vorfall:

Nach Ransomware-Angriff: Südwestfalen-IT und Kommunen lehnen Lösegeldzahlung ab

heise online | 10 days ago

Der kommunale **IT**-Dienstleister **Südwestfalen-IT** lehnt die Zahlung eines Lösegelds nach einem Ransomware-Angriff in Absprache mit den betroffenen Kommunen ab.

...rgruppe "Akira" steckt hinter

...IT hat eine hochprofessionelle ...genommen. Seit Tagen können ...gen nur sehr eingeschränkt

...IT: 72 Kommunen weiterhin lahmgelegt

...go

...e Cyberattacke mit Ransomware auf den **IT**-Dienstleister ...sorgt ...

WDR

Hackerangriff: Südwestfalen-IT räumt schwere Sicherheitslücken ein

Fast drei Monate nach dem Hackerangriff auf den Dienstleister Südwestfalen- IT ist klar: Der Hauptzugang des Unternehmens war einem...

vor 2 Wochen

WP.de

Cyberangriff in Siegen: „Die Südwestfalen-IT war deutlich zu optimistisch“

In Siegener Rathäusern denkt man nach Cyberattacke nun in längeren Zeiträumen. Laut Kreisverwaltung und SIT sei insbesondere die Koordination...

vor 1 Monat

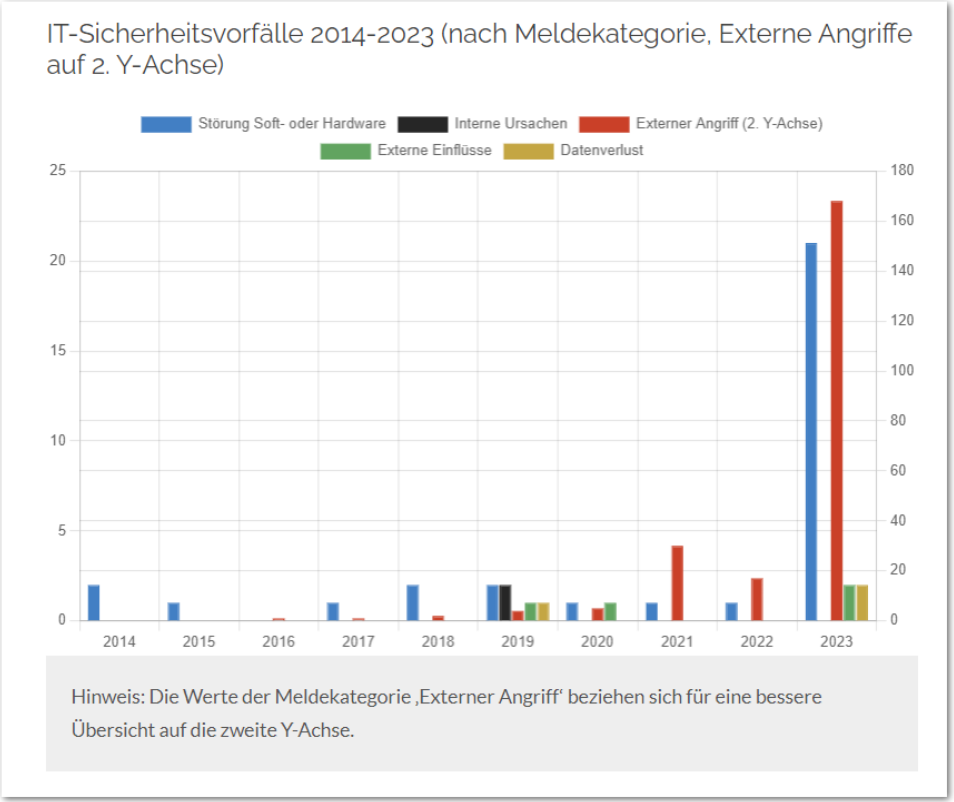
// Aktueller Fall: Kommunaler Notfallbetrieb – Angriff auf IT-Dienstleister mehrerer Kommunen in Südwestfalen

Es sind mehr als 115 Stadt-, Kreis- oder Gemeindeverwaltung im Regierungsbezirk Arnsberg, im weiteren Ruhrgebiet, im Rheinisch-Bergischen Kreis betroffen, dazu noch die Stadtverwaltungen von Borken, Ratingen und Schleiden, sowie die Stadt- und Kreisverwaltung Euskirchen betroffen.

Quelle: https://kommunaler-notbetrieb.de (Stand: 30.01.2024)

// Kommunale Notbetriebe: Übersichtskarte

Die Seite https://kommunaler-notbetrieb.de sammelt die Berichterstattung über IT-Sicherheitsvorfälle von Kommunalverwaltungen, die sich als Störungen, Notfälle und Krisen darstellen können.



// Kommunaler Notbetrieb in Westfalen-Lippe

Quelle: kommunaler-notbetrieb.de (Stand: 28.04.2023)

Kommunale Versorgungskassen Westfalen-Lippe

19.11.2024, PBR-Tagung im LWL-Schiffshebewerk Henrichenburg

Ein Ruf nach Rüstung: Wie schützen wir uns vor Cyber-Angriffen?

Nicklas Baier, Informationssicherheitsbeauftragter

// Im Zeitalter der Cyber-Schlachten: Die Rüstung - Ein Spiegelbild

// Agenda

- Einführung
- Die unsichtbare Bedrohung
- Zukunftsaussichten
- Fazit

// Bedrohung: Was ist ein Cyber-Angriff?

Ein Cyber-Angriff ist **ein Versuch**, Computer **außer Betrieb** zu setzen, **Daten zu stehlen** oder ein angegriffenes **Computersystem für weitere Angriffe** zu nutzen. Cyberkriminelle verwenden verschiedene Taktiken, um einen Cyber-Angriff zu starten, der **Malware, Phishing, Ransomware, Man-in-the-Middle-Angriffe** oder andere Verfahren einschließt.

// Vorsorge: Was ist Cyber-Sicherheit?

Cyber-Sicherheit ist der **Schutz kritischer Systeme** und **sensibler Informationen** vor digitalen und physischen Angriffen und Schäden. Cyber-Sicherheit ist ein Bestandteil der **IT-Sicherheit.** Sie bezieht sich auf die **Bekämpfung von Bedrohungen für vernetzte Systeme und Anwendungen**, unabhängig davon, ob diese Bedrohungen von **innerhalb oder außerhalb** einer Organisation ausgehen.

// Der Faktor Mensch

- In der IT-Sicherheit ist der Mensch oft das schwächste Glied. Trotz technischer Schutzmaßnahmen wie Firewalls und Verschlüsselung entscheiden menschliches Verhalten und Wissen über die Sicherheit. Phishing, Social Engineering und unbewusste Fehler zeigen: Der „Faktor Mensch“ ist entscheidend. Ohne Schulung und Bewusstsein sind selbst die besten Systeme angreifbar.
- Die Herausforderung besteht darin, Sicherheitsmaßnahmen so zu gestalten, dass sie effektiv sind, ohne die Benutzerfreundlichkeit zu opfern – sonst umgehen Mitarbeiter sie und gefährden so das System.

// Zusammenfassung: Cyber-Sicherheit ist das A und O

In einer zunehmend **vernetzten Welt** ist das Thema **Cyber-Sicherheit** von entscheidender Bedeutung. Die kvw und ihre Geschäftspartner sind zunehmend bedroht durch Cyber-Angriffe und müssen sich effektiv absichern, um ihre **Geschäftsprozesse aufrechterhalten** zu können.

Um den Schutz gegenüber Cyber-Angriffen zu gewährleisten, ist es wichtig, dass die kvw und ihre Mandanten ihre **Sicherheitsstrukturen kontinuierlich überprüfen und verbessern**. Eine einmalige Implementierung von Sicherheitsmaßnahmen ist nicht ausreichend, da **Bedrohungen ständig weiterentwickelt** werden.

// Agenda

- Einführung
- Die unsichtbare Bedrohung
- Zukunftsaussichten
- Fazit

// Bedrohung: Was ist ein Phishing?

Phishing ist eine **betrügerische Technik**, bei der Personen durch gefälschte Kommunikation dazu verleitet werden, vertrauliche **Informationen preiszugeben**, wie beispielsweise Passwörter, Kreditkarteninformationen oder persönliche Daten wie z.B. **Zugangsdaten**.

// Bedrohung: Was ist ein Ransomware?

Ransomware, auch Erpressungstrojaner, Erpressungssoftware, ist eine Form von **Schadsoftware**, die Daten auf einem Computer oder Netzwerk verschlüsselt und dann **Lösegeld** fordert, um die Daten wiederherzustellen.

// Nicht „Neu“: “Hände hoch! Dies ist ein Überfax!!“

- **Neue Kriminalitätsform:** Überfaxe bedrohen Unternehmen in Bremen – Täter fordern Geld per Telefax mit Drohung, das Fax-Gerät zu zerstören.
- **Angst um Geräte:** Aus Angst um teure Fax-Geräte sehen sich einige Opfer gezwungen, der Forderung nachzukommen.
- **Keine Schutzmaßnahmen:** Aktuell gibt es keinen wirksamen Schutz vor diesen Angriffen, die Polizei arbeitet aber an der Aufklärung.
- **Zukünftige Maßnahmen:** Die Bundespost entwickelt Systeme, um Faxe der Täter aufzuzeichnen und deren Identifizierung zu erleichtern.

Quelle: Taz, die Tageszeitung, Ausgabe 3266, 20.11.1990
https://taz.de/Haende-hoch-Dies-ist-ein-Ueberfax/!1743619/

// Vorsorge: Awareness Kampagnen & Phishing Kampagne

Awareness-Kampagnen zielen darauf ab, die **Sensibilisierung für Cyber-Bedrohungen zu erhöhen** und das Bewusstsein der Nutzer für potenzielle Gefahren wie Phishing-Kampagnen zu schärfen, um so ihre **Fähigkeit zu verbessern**, betrügerische Versuche zu erkennen und zu vermeiden.

// Zusammenfassung: Sensibilisierung in Worten

Der Schutz sensibler Daten ist sowohl im privaten als auch im Unternehmensumfeld unerlässlich, um Sicherheitsrisiken zu minimieren und das Vertrauen zu wahren.

Bewusster Umgang mit digitalen Tools und regelmäßige Sicherheitsupdates tragen entscheidend dazu bei, Systeme und Informationen nachhaltig zu sichern.

// Agenda

- Einführung
- Die unsichtbare Bedrohung
- Zukunftsaussichten
- Fazit

// Ausblick: Wie geht es weiter?

Die **Bedrohung durch Cyber-Angriffe** wird in Zukunft weiter **zunehmen**, da immer mehr Unternehmen und Geräte miteinander vernetzt werden.

Neue Technologien wie **künstliche Intelligenz (KI)** wird in Zukunft auch zur **Verbesserung der IT-Sicherheit** beitragen. Aber KI wird auch durch die Angreifer-Seite genutzt. Es bleibt abzuwarten, welche Entwicklungen die Zukunft bringen wird.

IT-Sicherheit erfordert sowohl im privaten als auch im Unternehmensumfeld ständige Aufmerksamkeit, regelmäßige Aktualisierungen und die Einhaltung bewährter Sicherheitsmaßnahmen, um Systeme und Daten dauerhaft zu schützen.

// Agenda

- Einführung
- Die unsichtbare Bedrohung
- Zukunftsaussichten
- Fazit

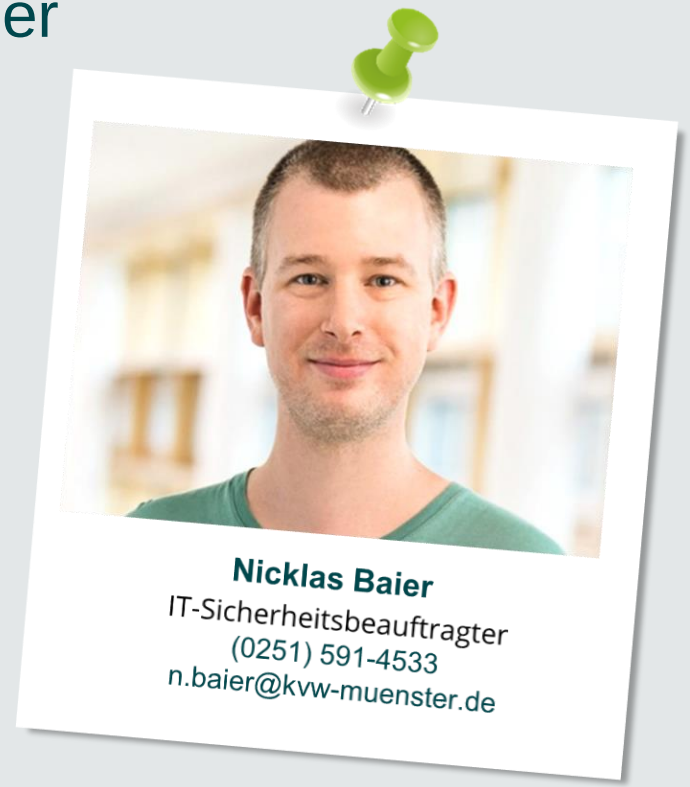
// Take aways: IT-Sicherheit ist kein Zustand, sondern ein Prozess

- In einer zunehmend vernetzten Welt ist IT-Sicherheit von entscheidender Bedeutung für den **Schutz der kvw, ihrer Mandanten und ihren Geschäftsprozessen**.
- Eine effektive IT-Sicherheitsstrategie erfordert eine **Kombination aus technischen und organisatorischen Maßnahmen** sowie ein **umfassendes Risikomanagement**.
- Es ist wichtig, kontinuierlich das **Sicherheitsniveau zu überprüfen und zu verbessern**, um sich vor den ständig weiterentwickelnden Bedrohungen zu schützen.

// Jeder kann ein Cyber-Ritter sein! - Auch Sie!

Jeder kann ein Cyber-Ritter sein, indem er sich über Sicherheitsmaßnahmen informiert, **starke Passwörter verwendet** und **andere über die Gefahren von Cyber-Bedrohungen aufklärt**. Gemeinsam können wir eine sicherere digitale Zukunft schaffen, in der jeder die Verantwortung übernimmt, unsere **virtuellen Räume zu schützen**.

// Ihr Ansprechpartner



Kommunale Versorgungskassen Westfalen-Lippe

Nehmen Sie mit:
Cyber-Sicherheit hat bei uns höchste Priorität!

Vielen Dank!