#ITkluggesichert

IT4B DIGITAL SUMMIT - CYBERSECURITY

HILFE - WURDEN WIR GEHACKT?

OLAF OTAHAL - SOLUTIONIT GMBH

HILFE - WURDEN WIR GEHACKT? - ZUR EINSTIMMUNG VORWEG…

- Wir als **solutionIT** beschäftigen uns seit fast 30 Jahren mit dem Thema IT-Sicherheit, um Daten (digitale Assets), Infrastrukturen und Menschen mit zeitgemäßen Produktlösungen zu sichern und unsere Kunden bei dieser Aufgabe zu unterstützen.

- IT-Sicherheit ist keine Frage der Notwendigkeit, sondern vielmehr die Frage der Wichtigkeit sowie Ernsthaftigkeit in Zeiten der digitalen Transformation.

- Bei Cyber-Angriffen (Incidents) stellte sich nicht die Frage, ob sie geschehen, sondern wann sie geschehen.

HILFE - WURDEN WIR GEHACKT? - AGENDA…

- Was passiert, wenn mein Unternehmen gehackt wurde?
- Welche Maßnahmen muss ich einleiten?
- Wie kann ich feststellen, ob mein Unternehmen gehackt wurde?
- Wie kann ich mein Unternehmen davor schützen?

HILFE - WURDEN WIR GEHACKT?

- **Was passiert, wenn mein Unternehmen gehackt wurde?**
  - Wenn ein Unternehmen gehackt wird, können die Angreifer auf vertrauliche Daten zugreifen, diese manipulieren oder löschen. Sie können Systeme lahmlegen und finanzielle Transaktionen kompromittieren. Häufige Folgen eines Hacks sind:
    - **Datenverlust und Datenlecks**: Persönliche und sensible Informationen von Kunden und Mitarbeitern können gestohlen und missbraucht werden.
    - **Finanzielle Verluste**: Direkte finanzielle Verluste durch Diebstahl oder Kosten für die Wiederherstellung und Reparatur können entstehen.
    - **Reputationsschaden**: Das Vertrauen der Kunden kann erheblich beschädigt werden, was langfristige Auswirkungen auf die Geschäftsbeziehungen haben kann.
    - **Betriebsunterbrechungen**: Systeme können lahmgelegt werden, was zu Produktionsausfällen und Einnahmeverlusten führt.
    - **Rechtliche Konsequenzen**: Je nach Art des Datenlecks können rechtliche Konsequenzen und hohe Bußgelder drohen.

HILFE - WURDEN WIR GEHACKT?

- **Welche Maßnahmen muss ich einleiten?**
  - Wenn Sie den Verdacht haben oder Sie feststellen, dass Ihr Unternehmen gehackt wurde, sollten Sie **sofort** folgende Schritte unternehmen:
    - **Vorfall melden und untersuchen:**
      - Melden Sie den Vorfall sofort an Ihre IT-Abteilung oder Ihren IT-Sicherheitsdienstleister.
      - Starten Sie eine gründliche Untersuchung, um das Ausmaß und die Art des Angriffs zu bestimmen.
    - **Systeme isolieren:**
      - Trennen Sie betroffene Systeme vom Netzwerk, um eine weitere Verbreitung des Schadens zu verhindern.
    - **Notfallplan aktivieren:**
      - Setzen Sie Ihren IT-Notfallplan in Kraft, falls vorhanden.
      - Informieren Sie alle relevanten Parteien, einschließlich Mitarbeiter, Kunden und ggf. Behörden.

HILFE - WURDEN WIR GEHACKT?

- **Welche Maßnahmen muss ich einleiten?**
  - Wenn Sie den Verdacht haben, dass Ihr Unternehmen gehackt wurde, sollten Sie sofort folgende Schritte unternehmen:
    - **Beweissicherung:**
      - Sammeln Sie alle möglichen Beweise für den Angriff, einschließlich Logfiles, E-Mails und Screenshots.
    - **Wiederherstellung und Bereinigung:**
      - Stellen Sie betroffene Systeme aus sauberen Backups wieder her.
      - Überprüfen und bereinigen Sie alle Systeme gründlich.
    - **Kommunikation:**
      - Informieren Sie Ihre Kunden und Partner transparent über den Vorfall und die ergriffenen Maßnahmen.
      - Arbeiten Sie mit PR-Experten zusammen, um den Reputationsschaden zu minimieren.

HILFE - WURDEN WIR GEHACKT?

- **Wie kann ich feststellen, ob mein Unternehmen gehackt wurde?**
  - Es gibt mehrere Anzeichen, die darauf hinweisen können, dass Ihr Unternehmen gehackt wurde:
    - **Ungewöhnliche Aktivitäten**: Beobachten Sie ungewöhnliche Anmeldungen, erhöhte Netzwerkaktivität oder unbekannte Prozesse auf Ihren Systemen.
    - **Veränderte oder gelöschte Daten**: Achten Sie auf unerklärliche Veränderungen oder das Verschwinden wichtiger Daten.
    - **Systemausfälle und -störungen**: Plötzliche Abstürze oder unerklärliche Fehlfunktionen können ein Hinweis sein.
    - **Warnungen von Sicherheitstools**: Nutzen Sie Sicherheitssoftware (Firewalls, Antivirenlösungen (besser EDR), Intrusion Detection Systeme, etc.), die auf verdächtige Aktivitäten hinweisen.
    - **Meldungen von externen Parteien**: Kunden, Partner oder Sicherheitsbehörden könnten Sie auf verdächtige Aktivitäten aufmerksam machen.

HILFE - WURDEN WIR GEHACKT?

- **Wie kann ich mein Unternehmen davor schützen?**
  - Um Ihr Unternehmen vor zukünftigen Hackerangriffen zu schützen, sollten Sie folgende Maßnahmen ergreifen:

    - **Sicherheitsrichtlinien und Schulungen:**
      - Entwickeln und implementieren Sie umfassende IT-Sicherheitsrichtlinien sowie achten Sie auf die Einhaltung.
      - Schulen Sie Mitarbeiter regelmäßig in Sicherheitsbewusstsein und im sicheren Umgang mit IT-Systemen.

    - **Technische Maßnahmen:**
      - Firewall und Antivirus-Software: Setzen Sie robuste Firewalls und aktuelle Antivirus-Software ein.
      - Sicherheitsupdates: Halten Sie alle Systeme und Software auf dem neuesten Stand, indem Sie regelmäßig Updates und Patches einspielen.
      - Verschlüsselung: Verschlüsseln Sie sensible Daten, sowohl bei der Speicherung als auch bei der Übertragung.

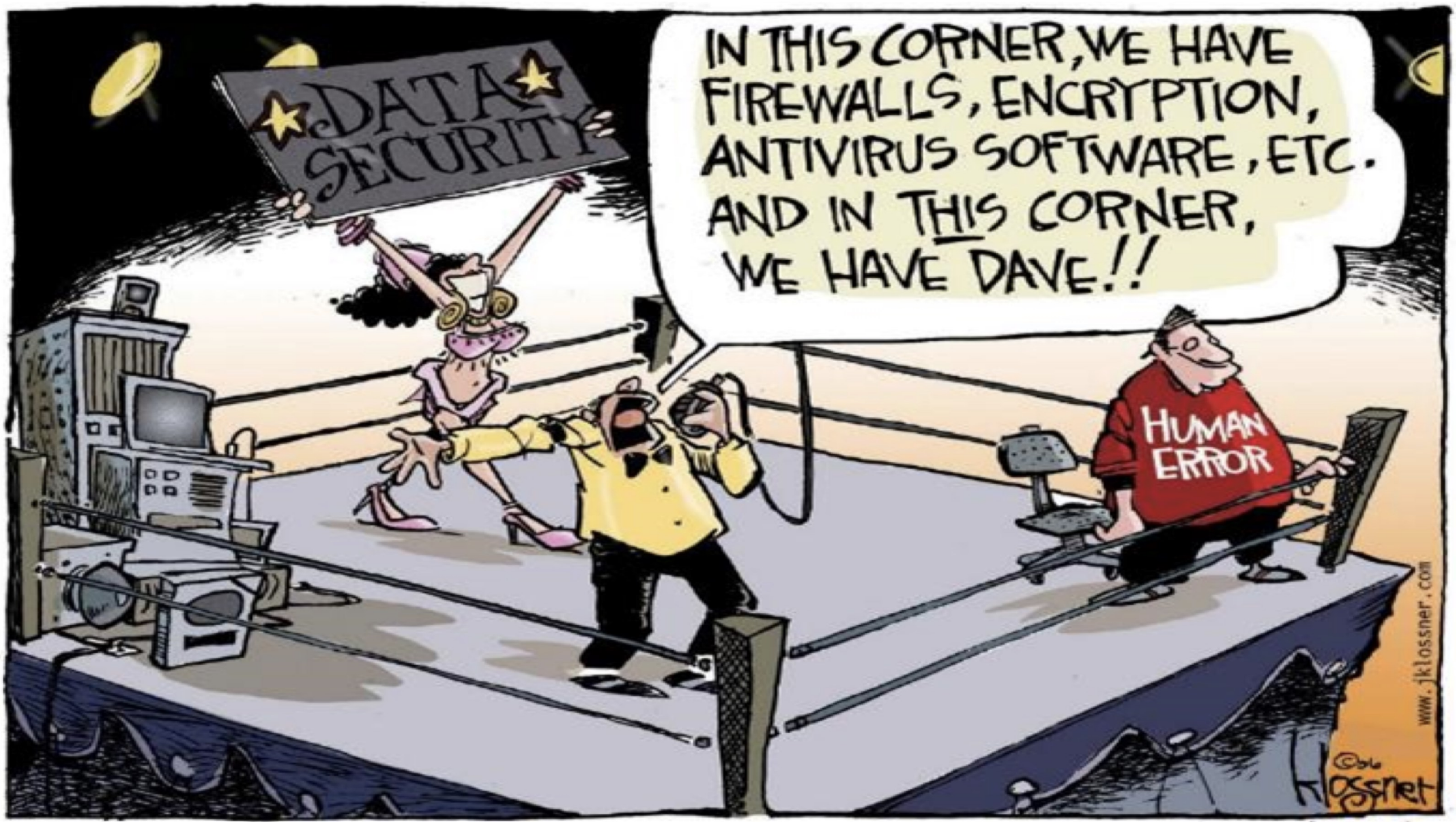
HILFE - WURDEN WIR GEHACKT?

- **Wie kann ich mein Unternehmen davor schützen?**
  - Um Ihr Unternehmen vor zukünftigen Hackerangriffen zu schützen, sollten Sie folgende Maßnahmen ergreifen:
    - **Zugangs- und Zugriffskontrollen:**
      - Starke Passwörter und Multi-Faktor-Authentifizierung - verwenden Sie komplexe Passwörter und setzen Sie Multi-Faktor-Authentifizierung ein.
      - Zugriffsrechte: Beschränken Sie den Zugriff auf vertrauliche Daten auf diejenigen Mitarbeiter, die diesen wirklich benötigen.
    - **Regelmäßige Sicherheitsüberprüfungen:**
      - Penetrationstests: Lassen Sie regelmäßig Penetrationstests durchführen, um Schwachstellen in Ihren Systemen zu identifizieren, sowohl von intern als auch von extern.
      - Sicherheitsaudits: Führen Sie regelmäßige Audits und Überprüfungen Ihrer Sicherheitsinfrastruktur und -maßnahmen durch.
    - **Notfall- und Wiederherstellungspläne:**
      - Erstellen und testen Sie Notfallpläne und Datenwiederherstellungsstrategien, um im Ernstfall schnell reagieren zu können.

HILFE - WURDEN WIR GEHACKT?

- Sicherheitslösungen müssen zu Ihrem Unternehmen passen, den notwendigen Schutz bieten, betreut werden und ihren Zweck erfüllen.

HILFE - WURDEN WIR GEHACKT?



HILFE - WURDEN WIR GEHACKT?

- Indem Sie die genannten Maßnahmen umsetzen, können Sie das Risiko eines Hackerangriffs erheblich reduzieren und die Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyberbedrohungen stärken.
- Denken Sie daran: IT-Sicherheit ist ein fortlaufender Prozess, der ständige Aufmerksamkeit und Anpassung erfordert.
- **Sie werden nie weniger Daten haben als heute.**
- **Datensicherheit ist keine Wahl mehr.**

Prinz William

HABEN SIE FRAGEN?

Besuchen Sie uns am Stand Nr. 9,

bei „MEET THE EXPERTS“ um 13:15 Uhr

oder unter

sicherheit-einfach-machen.com