Warum machen wir immer die gleichen Fehler?

Berichte aus dem Neuland IT-Security

#nuedigital

Daniel Jedecke

HISOLUTIONS

Über mich – Wer bin ich?

Daniel Jedecke (Senior Expert)

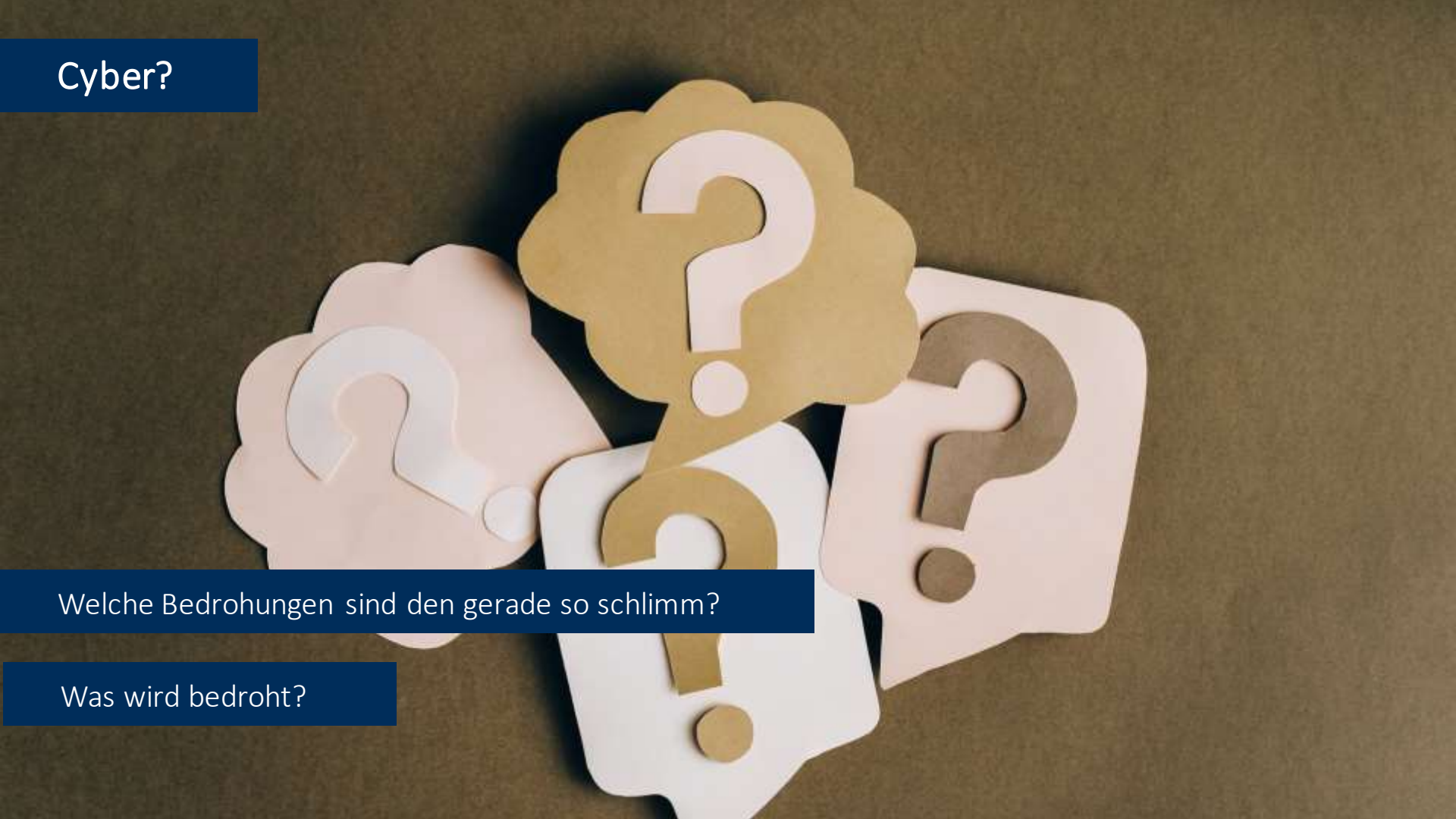
- Experte für Industrial IT und Forensik, Absolvent der TH Köln und RUB
- Ingenieur für Elektrotechnik
- Seit 7 Jahren bei der HiSolutions, über 20 Jahre in der IT Security
- Lehrbeauftragter
- Expertenwissen im Bereich Kritische Infrastrukturen, Cloud, Industrial Security und Incident Response
- Zertifizierungen (Auswahl):
  - Certified Lead Auditor ISO 27001
  - Certified Information Systems Auditor (CISA) & zertifizierter DSB
  - GIAC Defensible Security Architecture (GDSA) & Global Industrial Cyber Security Professional (GICSP)

Wir ermöglichen digitale Zukunft mit dem richtigen Zusammenspiel von Business, IT und Security.

Dafür gestalten wir mit Ihnen die benötigten Services, Architektur, Organisation, Arbeitsweisen und Arbeitsteilung – wirtschaftlich und sicher.

Oder wenn das Kind schon in den Brunnen gefallen ist, helfen wir Ihnen gerne wieder raus.

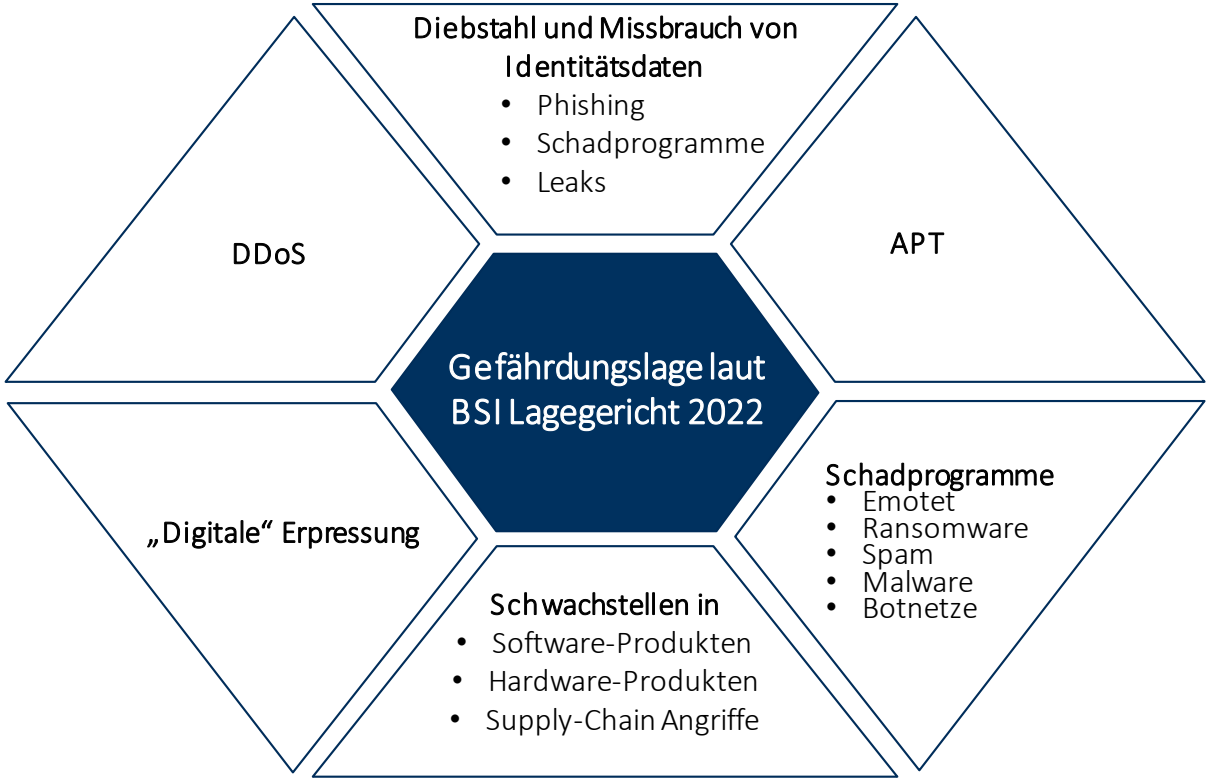
Cyber?



Welche Bedrohungen sind den gerade so schlimm?

Was wird bedroht?

Die Lage der IT-Sicherheit in Deutschland



Wer greift an

Staatsakteure

- Geopolitische Interessen
- Diebstahl von Wissen

Organisierte Kriminalität

- Phishing
- CEO Fraud
- Ransomware

Kleinkriminelle

- Abrechnungsbetrug

Wenn man dem Marketing traut …

- … braucht man folgende Dinge und alles ist gut
  - Next-Gen Firewall
  - Endpoint Protection
  - Awareness Schulungen
  - Cloud-Nutzung
  - CI/CD
  - SDWAN
  - MFA
  - Blockchain

  - Na, glauben Sie daran?

Ja aber …

- Die Maßnahmen sind gut aber man sollte wissen warum man diese einsetzt
- Zudem werden Sie keine Garantien bekommen das alle Angriffe abgewehrt werden können

- Und leider werden die ganzen Maßnahmen getrennt voneinander eingeführt und helfen oft nicht ganzheitlich

Machen wir also gerade alles neu?

- Nein!
- Wir Wettrüsten mit den Angreifern um Risiken zu eliminieren, welche wir eigentlich gar nicht haben müssten
- Beispiel:
  - Office Makros: Werden oft nicht genutzt aber werden nicht abgeschaltet. Daher schützt man sich durch Mail Appliances und Endpoint Protection
  - Operational Technology (OT): Wir verbinden die OT mit dem Office Netz um „Remote“ arbeiten zu können. Wir müssen dann wieder mehr Firewalls, Deep Inspection und ein zusätzliches Identity Management nutzen
  - Zero Trust: Früher war es Standard, das Daten in festen Formaten übertragen werden und validiert werden. Signaturen gab es auch vor 20 Jahren schon (Online Banking)

Warum gibt es oft Probleme

Die IT wächst ohne Struktur

Oft kommt „nur das billigste Angebot“ zum Zug

Externe Anforderungen fordern mehr Einsatz von IT (Ausschreibungen, Bestellungen, Kommunikation)

Meist macht jemand die IT „mit“

Man investiert in Hardware/Software-Lösungen statt in Wissen

Häufige Herausforderungen bei unseren Kunden

- Finanzielle Ressourcen
- Personelle Ressourcen
- Fehlende Awareness
- Mangelnde Dokumentation
- Bündelung auf Einzelne (Single-Point-Of-Failure)
- Fehlendes Krisenmanagement
- Steuerung der IT-Sicherheit bei externen Dienstleistern
- Fehlende Notfallstrategie

Nicht fragen OB wir gehackt werden sondern WANN

„Prävention und Reaktion“ sollten im Einklang stehen

Was sollte man also beachten

- Die „neuen“ Technologien zeigen uns auf, was wir früher schon mal gekonnt haben.
- Die Kernfrage bleibt aber: „Warum sichern wir Dinge ab, die man gar nicht braucht?“
- Ist uns also „Just-in-Time“ und „Immer und Sofort“ es wert, dass wir viel Geld in die IT-Sicherheit stecken müssen?

Muss es also immer was neues sein?

- Produkte helfen normalerweise nicht, IT-Sicherheit einzuführen. Sie unterstützen dies aber
- Beugen Sie dem Fall eines Einbruchs vor und haben Sie einen Plan
- Oft reicht es auch, bereits bekanntes erst mal umzusetzen (z.B. Office Makros abschalten)

Wo geht die Reise also hin?

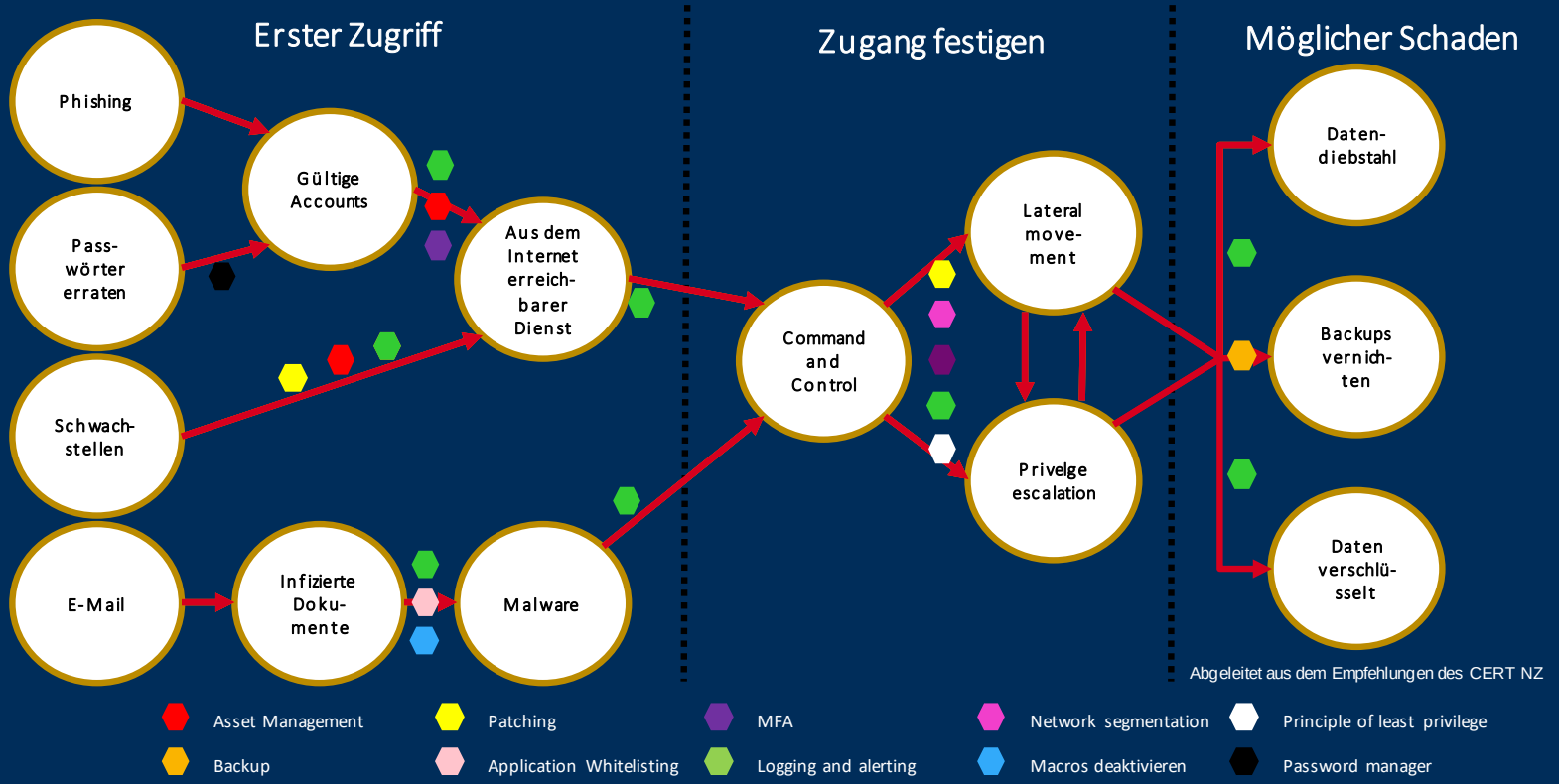
- Wir werden immer digitaler und müssen überlegen wie wir „mithalten“ können
- Wir müssen besser „kommunizieren“! Das Buzzword Bingo hilft nicht dabei, das IT-Sicherheit umgesetzt wird
- Gerade der Mittelstand versteht nicht mehr was er machen soll (und macht dann nichts)
- Wir müssen klar aufzeigen (auch gegenüber der Geschäftsleitung), welche Risiken die Wege beinhalten und dass man manche Wege dann besser nicht gehen sollte!

Wie denkt der Kopf?

- Das unbewusste System
  - arbeitet intuitiv und ohne aktive Steuerung
  - Beispiele: Autofahren, Radfahren
  - Oder automatisch Fehler auf dem Computer wegklicken ☺
- Das bewusste System
  - Wir denken über unser Handeln erst nach
  - Komplizierte Überlegungen sind möglich
  - Aber: Wir können uns nur noch auf dieses Problem konzentrieren
  - Kostet Zeit und aktives Teilhaben

Wir können daher Fehler gar nicht verhindern! Menschen machen Fehler. Wir müssen daher eine positive Fehlerkultur haben und Vorfälle schnell bearbeiten.

Abwehr!



Übersicht an Maßnahmen

- Mitarbeitersensibilisierung
- Identitäts- und Berechtigungsmanagement
- Multi-Faktor-Authentisierung (MFA)
- Passwortmanager
- Detektion und Reaktion
- Absicherung des Unternehmensnetzwerks
- Zeitnahes Patchen
- Absicherung der Clients und Sever
- Datensicherung
- Vorbereitung auf Sicherheitsvorfall
- Notfallmanagement

Folgekosten eines Vorfalls betragen ein vielfaches der Investitionen in Präventionsmaßnahmen.

Die beste Verteidigung ist nicht angegriffen zu werden!

Einfallstore absichern und abschrecken durch Vorbereitung, denn es wird primär nach einfachen Opfern gesucht.

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com

www.hisolutions.com