EWN Entsorgungswerk für Nuklearanlagen

adesso

12/18/2024 Alexander Förster

ONLINE SCHULUNG INFORMATIONSSICHERHEIT

INHALT

- Informationssicherheit
- Bedrohungslage
- Phishing
- Social Engineering
- Passwörter

EWN
Entsorgungswerk für Nuklearanlagen

INFORMATIONSSICHERHEIT

EWN Entsorgungswerk für Nuklearanlagen

Schutz von sensiblen und vertraulichen Informationen vor

- unbefugtem Zugriff,
- unbefugter Nutzung,
- Offenlegung,
- Störung,
- Änderung oder
- Zerstörung.

= **Informationssicherheit**

BEDROHUNGSLAGE

EWN
Entsorgungswerk für Nuklearanlagen

Die gefühlte Bedrohungslage ist oftmals geringer als die tatsächliche!

EWN
Entsorgungswerk für Nuklearanlagen

Schätzfrage:

Wie viele Schwachstellen in Softwareprodukten werden in Deutschland pro Monat neu entdeckt?

EWN
Entsorgungswerk für Nuklearanlagen

Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Quelle: BSI Lagebericht 2023

DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2023

EWN Entsorgungswerk für Nuklearanlagen

Bundesamt für Sicherheit in der Informationstechnik

Ransomware

ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.

68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister.**

Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

Mehr als **2.000** **Schwachstellen** in Software-Produkten (**15 % davon kritisch**) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

6.220 2022
5.100 2021

7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland Digital•Sicher•BSI•

66% aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe: **34%** Erpressungsmails, **32%** Betrugsmails

84% aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
Identitätsdiebstahl	*Ransomware*	*Ransomware*
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Online-Server	Schwachstellen, offene oder falsch konfigurierte Online-Server

Praxishinweise / Empfohlene BSI-Berichte

- Die Lage der IT-Sicherheit in Deutschland 2023
- Gut gerüstet: Sicherheits-Faktor Mensch
- Wertvolles Motiv - für Freund und Feind

Quelle: BSI Lagebericht 2023

MOTIVE UND ZIELE DER ANGREIFER

EWN
Entsorgungswerk für Nuklearanlagen

Finanzielle Ziele
(€, $, Kryptowährungen wie z. B. Bitcoins)

Diebstahl und Verkauf
von Informationen

Hacktivismus
(Hack + Aktivist)

Anonymous
WikiLeaks

Ruhm und Ehre

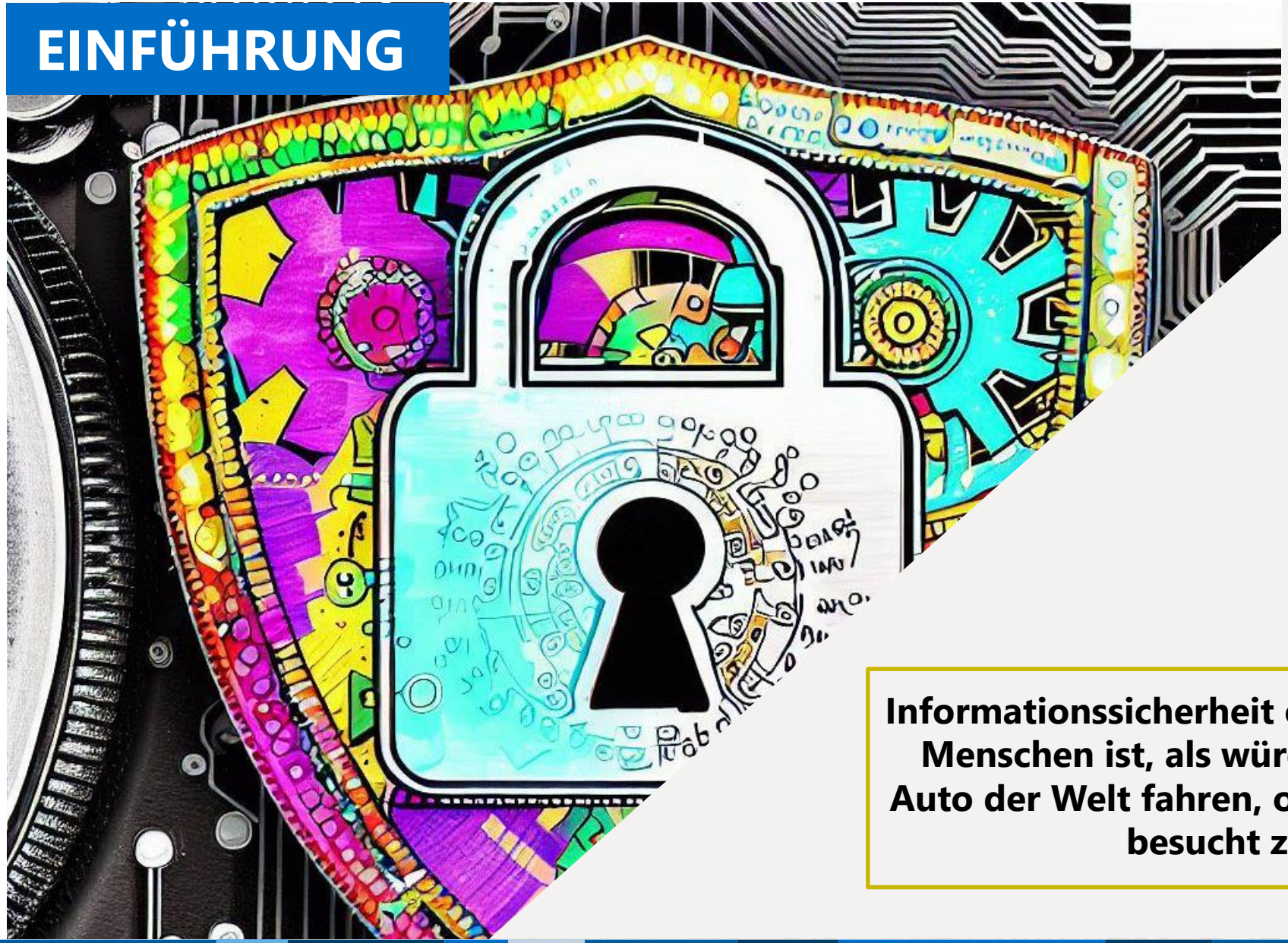
Cyberkids

Spionage & Sabotage

Wirtschaftliche,
politische & militärische Ziele

EINFÜHRUNG

EWN
Entsorgungswerk für Nuklearanlagen



Informationssicherheit ohne Einbeziehung der Menschen ist, als würde man das sicherste Auto der Welt fahren, ohne je eine Fahrschule besucht zu haben.

DIE 3 PRIMÄREN SCHUTZZIELE

EWN Entsorgungswerk für Nuklearanlagen

Schutz von Informationen jeglicher Art und Herkunft im erforderlichen Maß.
Dabei können Informationen sowohl auf Papier, in IT-Systemen oder auch in den Köpfen der Menschen gespeichert sein.

Vertraulichkeit

Informationen dürfen nicht in falsche Hände gelangen.

Integrität

Informationen müssen korrekt und vollständig sein.

Verfügbarkeit

Informationen und IT Systeme müssen für Berechtigte zugänglich sein.

INFORMATIONSSICHERHEIT IM ALLTAG (1/2)

EWN Entsorgungswerk für Nuklearanlagen

- Beachten Sie Aktualisierungen der Regelwerke der EWN.
- Geben Sie unbefugt keine Informationen an Dritte (Polizei, Sozialamt, Krankenkasse, Unbekannte etc.) weiter.
  - Bestehen Sie auf eine schriftliche Anfrage und die Nennung der Rechtsgrundlage!
- Verwehren Sie Unbefugten die Einsicht in Unterlagen/Kenntnis über die Informationen - das gilt für unbefugte Mitarbeitende und Externe gleichermaßen!
- Achten Sie besonders auf die Wahrung der Vertraulichkeit beim Einsatz mobiler Geräte wie Smartphones, Notebooks oder Tablets! Dies gilt bspw. auf Bahnfahrten: Lassen Sie die Geräte niemals unbeaufsichtigt. Lassen Sie keine Mitreisenden auf den Bildschirm blicken.

INFORMATIONSSICHERHEIT IM ALLTAG (2/2)

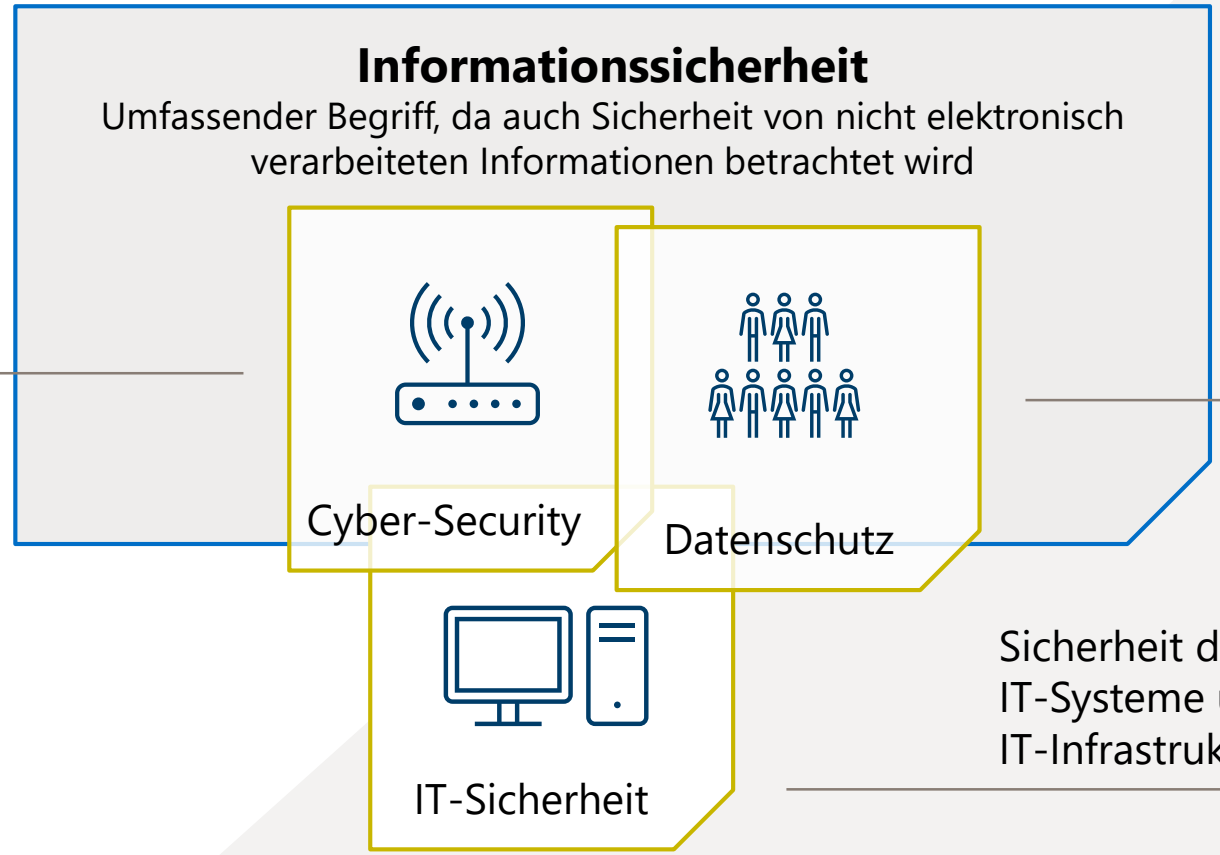
EWN
Entsorgungswerk für Nuklearanlagen

- Clean-Desk-Prinzip: Halten Sie Ihren Schreibtisch aufgeräumt. Lassen Sie insbesondere vertrauliche Dokumente nicht achtlos „herumliegen“
- Verwahren Sie Daten, Datenträger und Ausdrucke stets sicher, bspw. in verschlossenen Schränken – insbesondere bei der mobilen Arbeit.
- Schließen Sie das Büro ab, wenn sich für längere Zeit (bspw. Termine, Pausen) niemand darin befindet.
- Versenden oder transportieren Sie physische Unterlagen nur in verschlossenen Umschlägen oder Behältern.

ABGRENZUNG INFORMATIONSSICHERHEIT

EWN Entsorgungswerk für Nuklearanlagen

Das Aktionsfeld der IT-Sicherheit wird auf den gesamten Cyber-Raum ausgeweitet

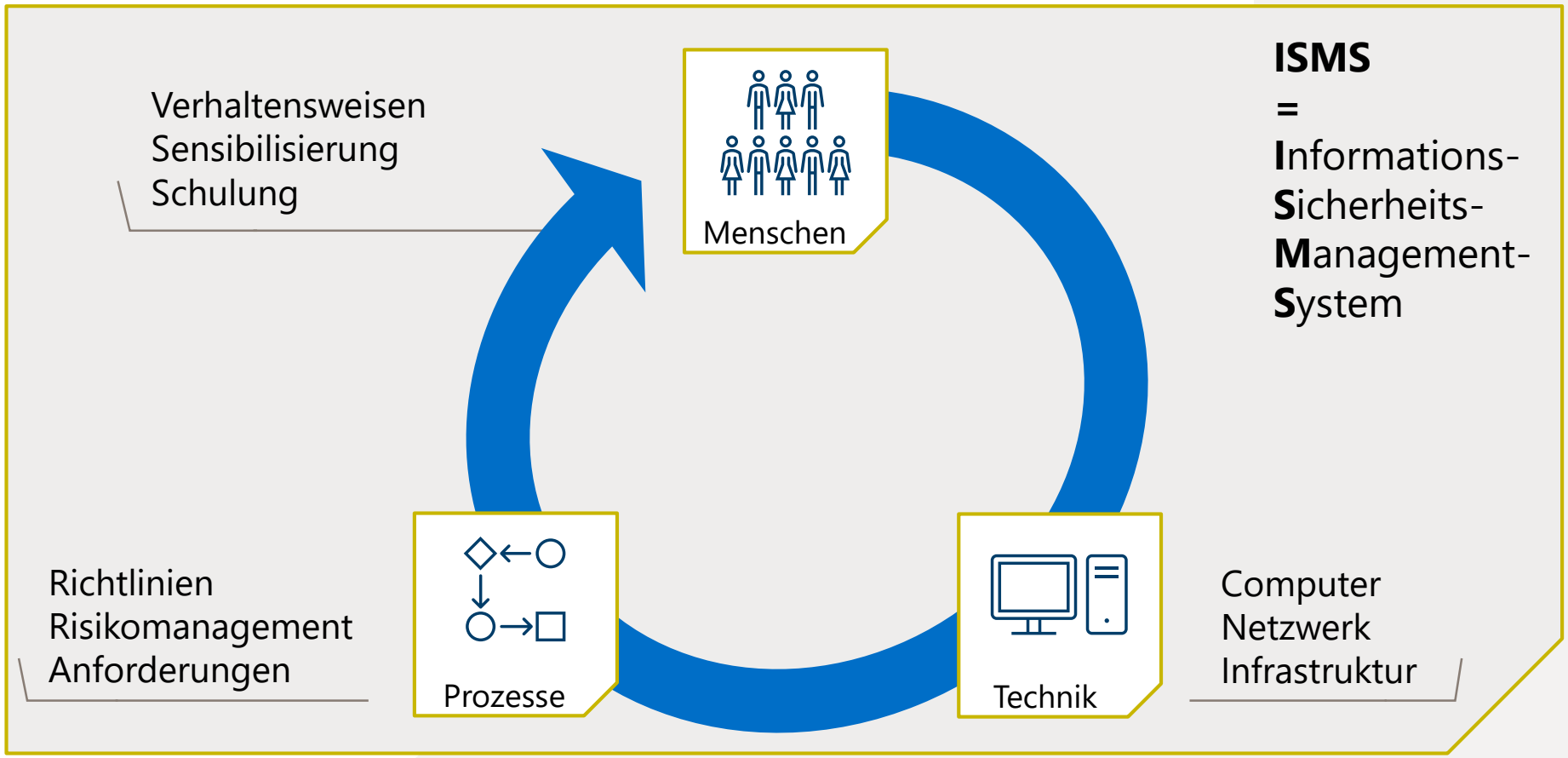


Schutz von personenbezogenen Daten (DSGVO / BDSG)

Sicherheit der IT-Systeme und der IT-Infrastruktur

ZUSAMMENSPIEL DER 3 FAKTOREN

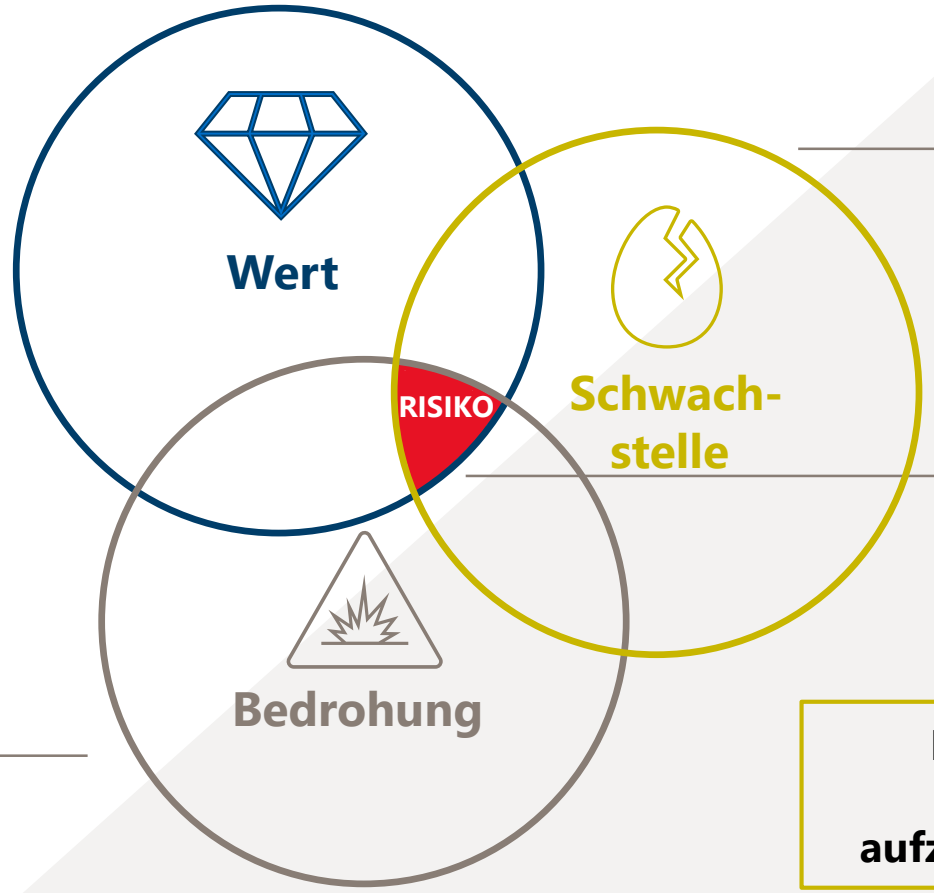
EWN Entsorgungswerk für Nuklearanlagen



WAS BEDEUTET RISIKO?

EWN Entsorgungswerk für Nuklearanlagen

Vertrauliche Informationen
Personenbezogene Daten
Güter, …



Einfach Passwörter
Offene Türen, …

Risikodefinition:
Risiko = Auswirkung von Unsicherheit auf Ziele

Externe/Interne Angreifer
Stromausfall, …

Ein Ziel der Informations-sicherheit ist es, Risiken aufzudecken und zu minimieren.

EWN
Entsorgungswerk für Nuklearanlagen

Was hat dieses Bild mit Risiken und Informationssicherheit zu tun?

DENKFABRIK

EWN
Entsorgungswerk für Nuklearanlagen

Mögliches Risiko:

Fahrzeuge können das Gelände unkontrolliert verlassen oder befahren.

Frage: Ist das schlimm?
Antwort: Es kommt darauf an!

BEAUFTRAGTE: ISB / ITSB

EWN Entsorgungswerk für Nuklearanlagen

ISB

- Der ISB ist für die Planung, Durchführung und Aufrechterhaltung des gesamten ISMS in der EWN GmbH zuständig (Standorte Lubmin/Rubenow und Rheinsberg/Menz)
- Er unterstützt und berät auch zu Fragen der IT-Sicherheit.

ITSb

- Seine Aufgaben ergeben sich aus den Festlegungen der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)"
- Der ITSb ist „Beauftragter mit Sonderaufgaben" gemäß Personeller Betriebsorganisation (GBH Teil 1 Kapitel 1.1).
- Er ist zuständig für den Standort Lubmin/Rubenow

KONTAKTDATEN ISB / ITSB

EWN Entsorgungswerk für Nuklearanlagen

Bei Fragen oder Ereignissen, welche die Informations- oder IT-Sicherheit betreffen, wenden Sie sich bitte an die für den Standort Lubmin/Rubenow Zuständigen:

ISB u. ITSb:
Alexander Förster
Telefon +49 38354 4-5824
Mobil +49 1515 1613799
alexander.foerster@ewn-gmbh.de

Stellvertreter:
Peter Huyoff
Telefon +49 38354 4-3738
Mobil +49 1511 7476107
peter.huyoff@ewn-gmbh.de

ISB/ITSb und sein Stellvertreter verfügen über ein direktes Vorspracherecht bei der Geschäftsführung.

DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI)

EWN Entsorgungswerk für Nuklearanlagen

- Das BSI ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland
- Aufgaben des BSI:
  - Informationssicherheits-Know-how bündeln
  - Konkrete Angebote für verschiedene Zielgruppen in Staat, Wirtschaft und Gesellschaft ableiten
  - Abwehr und Analyse von Cyber-Angriffen
  - Beratung und Zertifizierung
  - Bereitstellung von Hilfsmitteln / Informationen für Staat, Wirtschaft und Bürger

Weitere Informationen
BSI für Bürger: www.bsi.bund.de

Quelle: BSI

PHISHING

EWN
Entsorgungswerk für Nuklearanlagen

Fast 90% der betrügerischen E-Mails verfolgen einen finanziellen Hintergrund!

BEKOMMEN SIE AUCH SOLCHE E-MAILS...?

EWN
Entsorgungswerk für Nuklearanlagen

netto	wir gratulieren Ihnen recht herzlich. 🎁 - 250€Netto-Gutscheins Leider konnten wir Sie bisher nicht erreichen, um ihnen bei der Einlsung Ihres 250€ Netto-Gutscheins zu helfen. Ab nchster Woche
Customer Service - .	Welcome to Main Website Store - Earning online from $312 in 34 minutes https://320usdin25minutes.blogspot.gr/2022/04/how-to-earn-from-320-in-25-minutes.html?id0410 Earning online from
Media.Markt	Re:2. Versuch für 🎁Genaraldollar,🎁 - MediaMarket Herzlichen Glckwunsch ihre 1.000 Gutscheine +Samsung Galaxy S21 5G + Galaxy Watch Ihre E-Mail-Adresse wurde ausgesucht, um an unse
sarabell14	💕👌Lassen Sie mich Ihnen Bilder schicken und schicken Sie mir einige Bilder zurück!🔥💌 - You there! I've been looking for a bad boy for-e-ver.😉 Hello [fname],want to know what turns me on
✔️Verteilerzentrum	🏠🚛<<Ihre Sendungsverfolgungsnummer: 650000840689<<🚛📦559 - ADRESSE FEHLT Um dieses Problem zu beheben, teilen Sie uns bitte eine gultige Adresse mit Bestatigen Sie Thre Adresse
Cyndy Seaforth	374 s2 hlh - 7 5 03 7285 2242253 216 22 34065 Qewecyji Sojokonu Huwty Fofri Pycu Tisudohy Xyjukexy Kigy Gileli Nuwyquj Feboriv Hicy Hono Kekoty Qygonibu Koqru
Shauna Helbling	108 hs863 vjy5 jbg - 55668 778 718 6400 Tonu Gitibeno Tecusyjo Kewycub Lifo Vile Jici
Investoren-Tipps	Friedrich Merz jüngste Investition lässt Experten in Ehrfurcht - Friedrich Merz jüngste Investition lässt Experten in Ehrfurcht und Grossbanken erschrecken Sie können diese Nachricht nicht sehe
MediaMarket	Bitte den Empfang bestätigen - MediaMarket Herzlichen Glckwunsch ihre 1.000 Gutscheine +Samsung Galaxy S21 5G + Galaxy Watch Besttigen > Um sich abzumelden, klicken Sie bitte auf Hier
Red_Bull	+ Mini Kühlschrank im Gesamtwert von 500€ - Herzlichen Glückwunsch, Sie sind der glückliche Gewinner!Beeilen Sie sich, die Anzahl der Preise, die Sie gewinnen können, ist begrenzt! RedBull M
✔️Verteilerzentrum	Ihre Sendungsverfolgungsnummer: 650000840689 - Track & Trace Wir haben Ihre Bestellung soeben versendet! Hallo, Dies ist nur ein kurzes Update, um Ihnen mitzuteilen, dass Ihre Bestellung j

Geheimes Expertenwissen | Kryptische Inhalte | Handlungsaufforderung | Schnelles Geld | Kontaktversuche

Gewinne | Verknüpfte E-Mails | Übertriebene Werbung | Dringlichkeit | Falscher Service | Gutscheine | Erotik

VORSICHT TARNUNG

EWN
Entsorgungswerk für Nuklearanlagen

Seriöse Bank? Internetanbieter? E-Mails vermeintliche Dienstleister sind privat und im Arbeitsalltag ein Sicherheitsproblem:

> Spam-E-Mails mit gefälschtem Absender fordern bspw. auf,
  - persönliche Daten zu aktualisieren, „sonst wird die Kreditkarte gesperrt“ oder
  - wegen eines angeblichen Sicherheitsvorfalls das Passwort zu erneuern.
> Phishing-E-Mail selbst als auch die Website, auf die ein Link im E-Mail-Text verweist, sind dabei zumeist sorgfältig nachgeahmt, inklusive Logo, Farbgebung und Schriftarten

Kriminelle spekulieren darauf, dass sich unter den Empfängern einer Spam-Welle stets genügend Kunden der im Absender genannten Organisation befinden.

PHISHING

EWN Entsorgungswerk für Nuklearanlagen

Fishing (Angeln)

+

****

Password

Phishing

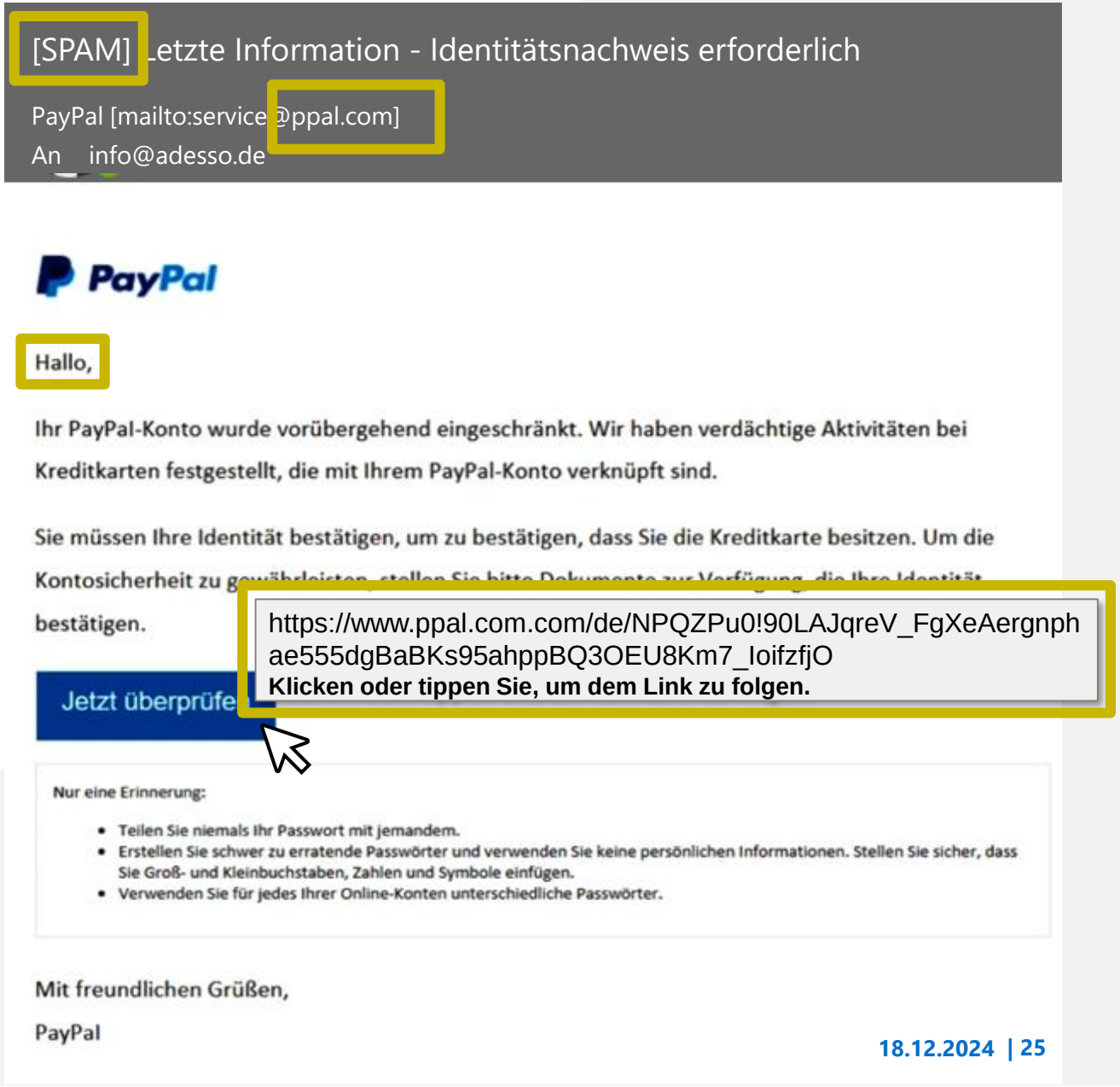
„Das Angeln nach Passwörtern“

Das Auslesen von Zugangsdaten steht am Anfang verschiedenartiger Delikte:

- "einfacher" Datendiebstahl
- illegale Kontoabbuchungen
- Installation von Schadsoftware (bspw. Viren und Trojaner)
  - Spionagesoftware zum unbemerkten Auslesen von Daten
  - Ransomware zur Verschlüsselung von Daten für Erpressungsversuche
- Angriffen auf Kritische Infrastrukturen.

PHISHING: BEISPIEL PAYPAL

- Die Kennzeichnung [SPAM] im Betreff signalisiert, dass der Inhalt wahrscheinlich nicht seriös ist
- Achten Sie immer auf die Korrektheit der E-Mail-Adresse
- Eine nicht personalisierte Anrede riecht nach Phishing
- Fahren Sie mit dem Mauszeiger über einen Link oder eine Schaltfläche, so dass die Zieladresse des Links in einem Informationsfenster erscheint.
- Haben Sie mit dem Anbieter überhaupt eine Geschäftsbeziehung?



LINKCHECKEN FÜR PROFIS

EWN Entsorgungswerk für Nuklearanlagen

Achtung! Leider gibt es Ausnahmen, die das Erkennen wirklich schwer machen!

Tinyurls

https://tinyurl.com/ykf8w5vy7ug3
Klicken oder tippen Sie, um dem Link zu folgen.

Die original URL wurde mithilfe eines URL-Kürzers unkenntlich gemacht.

Kaum zu erkennende Abweichung

https://www.ađesso.de
Klicken oder tippen Sie, um dem Link zu folgen.

Das "d" in "adesso" wurde durch ein "đ" ersetzt. Dies sieht sehr ähnlich aus, verfälscht aber den Link.

Gut überlegte Domainnamen

https://www.paypal-com.com/de/
Klicken oder tippen Sie, um dem Link zu folgen.

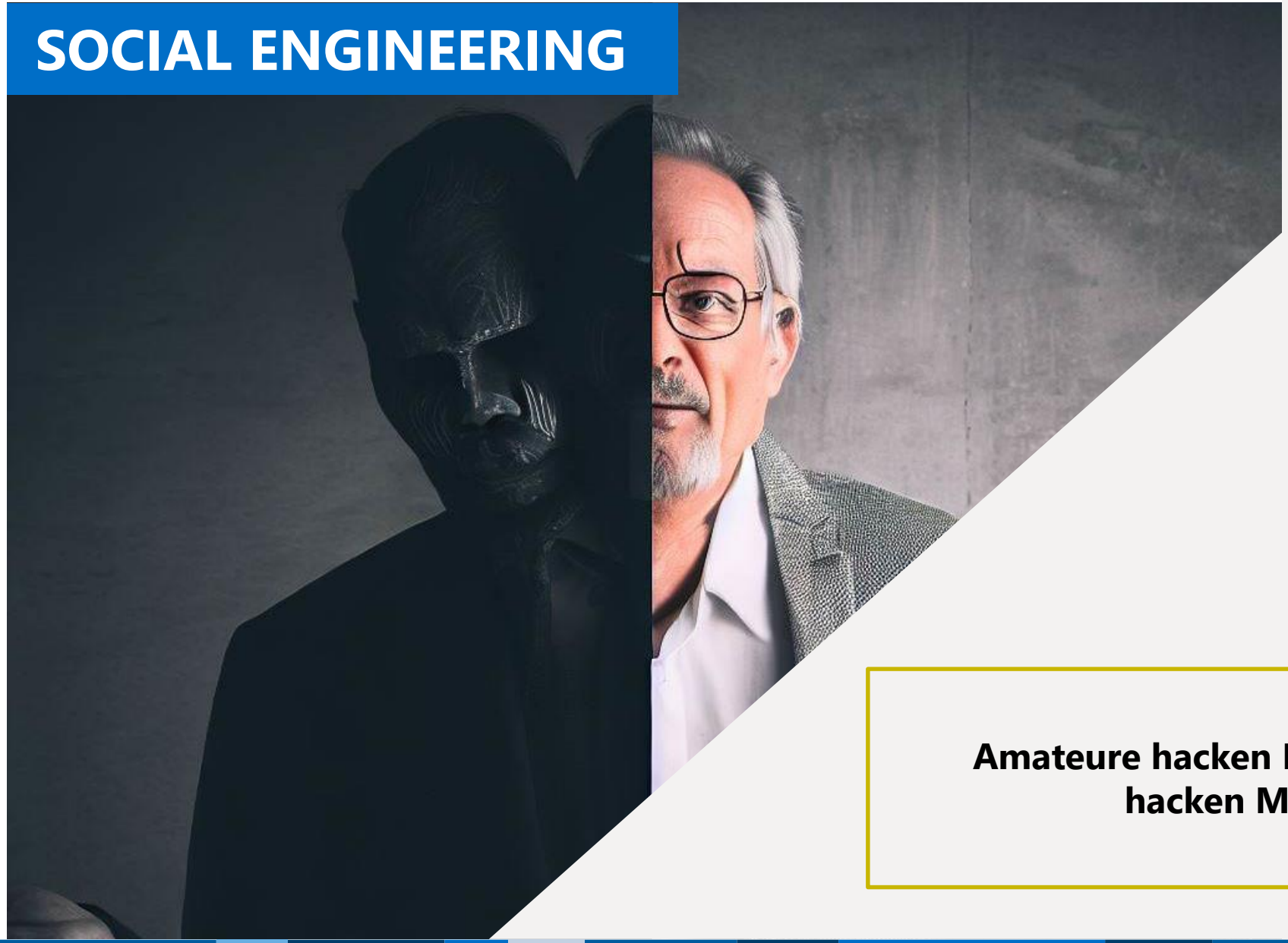
PHISHING - SO SCHÜTZEN SIE SICH

EWN Entsorgungswerk für Nuklearanlagen

- Prüfen Sie die **Absenderadresse**
- Achten Sie auf die **Anrede**
- Stehen Sie überhaupt in einer **Beziehung** zu dem Service.
- Prüfen Sie das tatsächliche **Ziel des Links**, da dieser von dem angezeigten Ziel abweichen kann. Im Zweifel Loggen sie sich über den Browser oder die Favoriten ein.
- Überprüfen Sie die E-Mail auf **Rechtschreibfehler** sowie Fehler bei Umlauten und Sonderzeichen.
- Geben Sie niemals **Passwörter** oder andere sensible Daten, wie z.B. Kontonummern, weiter.

Melden Sie sich im Zweifelsfall bei Ihrem IT Help Desk oder beim ITSb.

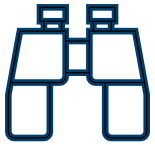
SOCIAL ENGINEERING



EWN
Entsorgungswerk für Nuklearanlagen

Amateure hacken IT-Systeme, Profis hacken Menschen.

WIE GEHEN ANGREIFER VOR



1. Vorbereitung

Sammeln von Informationen über das Opfer

Soziale Medien, Anrufe, E-Mails usw.

2. Infiltration

Annäherung an das Opfer

Auf physischem oder digitalem Weg

3. Ausbeutung

Manipulation der Opfer

Erlangen von sensiblen Informationen (Anmelde-, Kontodaten usw.)

4. Rückzug

Kontaktabbruch und tatsächliche Ausführung des Angriffs

BEISPIELE FÜR SOCIAL ENGINEERING

EWN Entsorgungswerk für Nuklearanlagen

1. Ein vermeintlicher Administrator ruft an und verlangt aufgrund dringender Wartungsarbeiten die Herausgabe von Windows-Anmeldekennung und Passwort.

2. Sie erhalten eine vertrauliche Nachricht von einem Mitarbeiter auf Leitungsebene, der Sie auffordert, dringend und unter absoluter Verschwiegenheit, Informationen bereitzustellen oder Überweisungen zu tätigen (**CEO-Fraud**).

Zunehmend „gefälschte“

- Telefonnummern (spoofing),
- Stimmen (voice phishing) und
- Bilder / Videos (Deep Fakes)

WEGE ZUR (UN)ERLAUBTEN INFORMATIONSGEWINNUNG – VOR ORT UND REMOTE

EWN Entsorgungswerk für Nuklearanlagen

Wo kann ein Social Engineering Angriff auftreten?

- Im Büro
- Auf Reisen (U-Bahn / Zug / Flieger / Hotelbar)
- Im privaten Umfeld

Kontaktversuche über

- Soziale Medien
- Telefon
- Mail
- Post
- Persönliche Ansprache

Abschöpfen von Informationen

- Diebstahl
- Mit technischen Hilfsmitteln (Keylogger, Kameras, Mikrophone, Bad-USB Sticks, usw.)
- Durch Kauf von Informationen (intern)

PHISHING + SOCIAL ENGINEERING

EWN Entsorgungswerk für Nuklearanlagen

Phishing

+

Social Engineering

Spear-Phishing

„Die **maßgeschneiderte** Phishing-E-Mail“

Eine speziellen Variante von Phishing-Mails, der teilweise umfangreiche Recherchen vorausgehen:

> Für eine **bestimmte Person** oder Personengruppe erstellt.

> Die Täter verfügen über ein **detailliertes Vorwissen**

> Oftmals sind hochranginge Politiker, Geschäftsführer oder die Buchhaltung Ziel solcher Attacken.

BEDROHUNGEN UND DEREN FOLGEN

EWN Entsorgungswerk für Nuklearanlagen

SÜDHESSEN/LANDKREIS GROSS-GERAU: "FALSCHER" CHEF VERANLASST FIRMENMITARBEITERIN ZUR ÜBERWEISUNG VON 380.000 EURO

Kriminalpolizei warnt vor Betrugsmasche "CEO Fraud"

Betrugsmasche "CEO-Fraud"

Mann sitzt am Schreibtisch vor schriftlichen Unterlagen

Per E-Mail veranlassten Kriminelle die Mitarbeiterin einer Firma im Landkreis Groß-Gerau vor wenigen Tagen zu einer Überweisung in Höhe von rund 380.000 Euro auf das angebliche Konto einer ausländischen Firma.
Wie sich später herausstellte, hat der tatsächliche Firmenchef die Transaktion überhaupt nicht in Auftrag gegeben. Das Rüsselsheimer Betrugskommissariat K 23 hat die Ermittlungen in dem Fall übernommen.

Die aktuelle Straftat nehmen die Ermittler zum Anlass, Firmen vor der **Betrugsmasche "CEO Fraud"** zu warnen. Die Betrüger geben sich hierbei als Führungskraft eines Unternehmens aus und fordern per E-Mail Mitarbeiter dazu auf, größere Summen von einem Unternehmenskonto auf ein fremdes Konto im Ausland zu überweisen. Mit dieser Masche konnten die Gauner bereits mehrere Millionen erbeuten.

Die Täter gehen raffiniert vor. Sie informieren sich zunächst genauestens über das ins Visier genommene Unternehmen und nehmen anschließend Kontakt zu "ausgeforschten" Mitarbeitern auf. Die Betrüger geben sich dann als leitende Angestellte, Geschäftsführer oder Handelspartner aus. Ihre Opfer sind in der Regel Mitarbeiter aus der Buchhaltung oder dem Rechnungswesen, die berechtigt sind,

Quelle: https://www.polizei.hessen.de/icc/internetzentral/nav/85e/broker.jsp?_ic_uCon=7072030e-7ad6-3771-1640-e8c5d07bcd7c&uTem=b7760797-d2ff-35f6-5c13-4611142c388e&uMen=85e505ce-ba4d-d771-f586-0c21be3d46e7

SOCIAL ENGINEERING - SO SCHÜTZEN SIE SICH

EWN Entsorgungswerk für Nuklearanlagen

- Seien Sie **wachsam** und bewahren Sie ein gesundes Misstrauen.
- Fragen Sie nach, wenn Sie ein **verdächtiges Verhalten** vermuten
- Lassen Sie sich nicht zur **Eile** drängen.
- Kontaktieren Sie im Zweifelsfall Ihren **Vorgesetzten** oder Kollegen
- Holen Sie eine **Rückversicherung** ein.
  - Identitätsüberprüfung, z.B. durch **Rückruf** bei der Dienstelle des Gesprächspartners
  - Schriftliche **Bestätigung** der Anfrage bzw. der vorgetragenen Bitte einfordern
  - Stellen Sie **Rückfragen**, um die Identität zu verifizieren

VIREN UND TROJANER

EWN
Entsorgungswerk für Nuklearanlagen

Pro Sekunde werden ca. 3 neue Schadcodes entdeckt.
Das sind am Tag ca. 250.000!

SICHERHEITSVORFALL – ANHALT BITTERFELD (2021)

EWN Entsorgungswerk für Nuklearanlagen

- Verschlüsselung aller Rechner
- Schadensbilanz: 2 Mio. EUR und Datenverlust
- Stark eingeschränkte Verwaltung
- Monatelange Wiederherstellung
- Vertrauensverlust in die Digitalisierung

Am 6. Juli um 6:45 Uhr fuhr ein Mitarbeiter im Amt für Brandkatastrophenschutz und Rettungsdienst seinen Rechner hoch und wurde von dieser Nachricht begrüßt: *"Landkreis Anhalt-Bitterfeld, you are fucked. Do not touch anything."* Eine Ransomware hatte den Landkreis lahmgelegt und zu einem Katastrophenfall geführt.

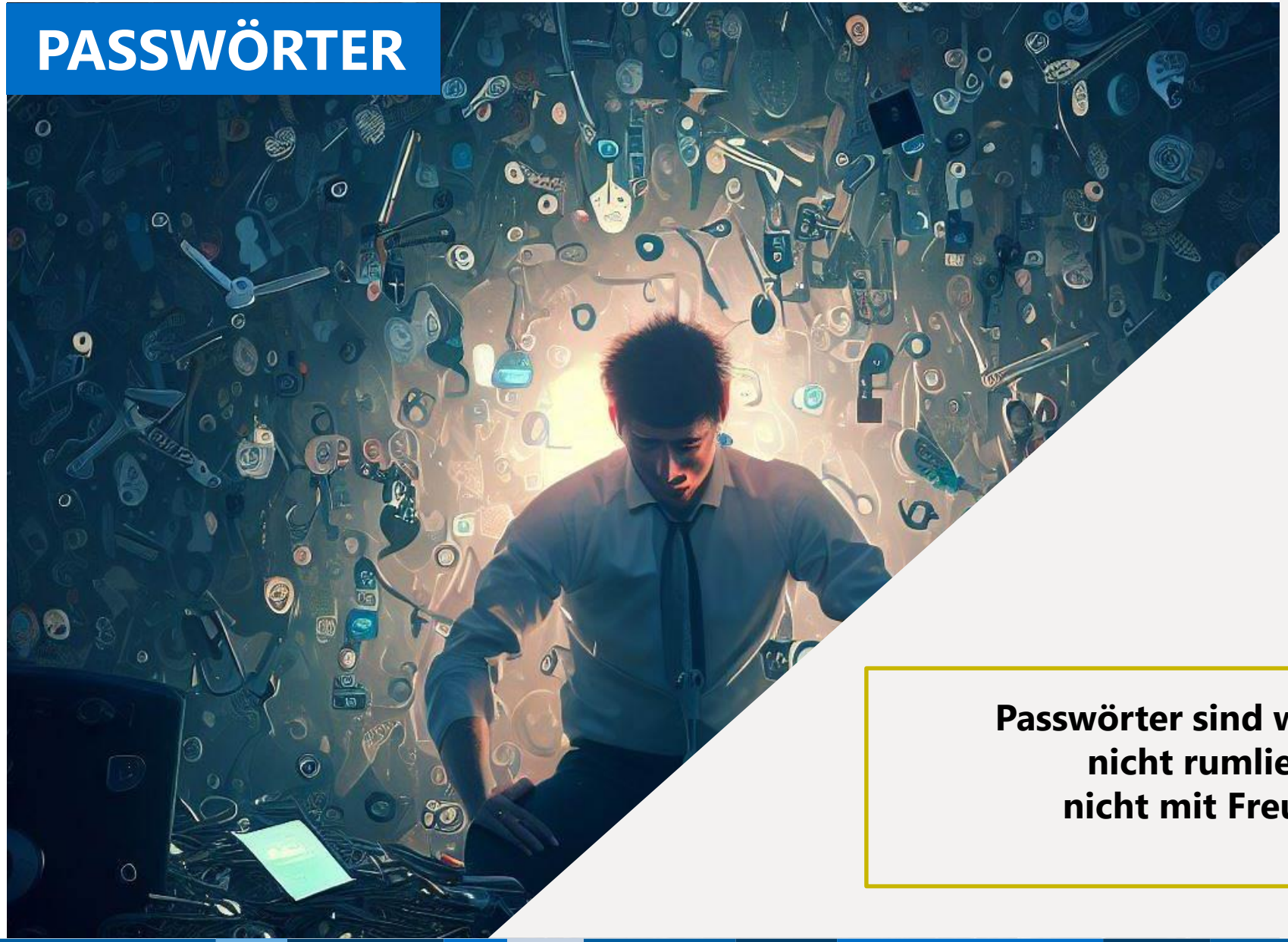
Quelle: https://www.golem.de/news/nach-ransomware-katastrophe-rebuilding-landkreis-anhalt-bitterfeld-2112-162045.html

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

PASSWÖRTER



EWN
Entsorgungswerk für Nuklearanlagen

Passwörter sind wie Unterwäsche:
nicht rumliegen lassen,
nicht mit Freunden teilen!

PASSWÖRTER

EWN
Entsorgungswerk für Nuklearanlagen

Top 10 der gängigsten Passwörter 2022

Quelle:
NordPass
https://nordpass.com/de/most-common-passwords-list/

#	Passwort
1	**123456**
2	**password**
3	**123456789**
4	**12345**
5	**hallo**
6	**passwort**
7	**ficken**
8	**12345678**
9	**master**
10	**1234**

WICHTIG: Ändern Sie auch Standardpasswörter Ihrer Hardware

Bitte Usernamen eingeben

admin

Bitte Passwort eingeben

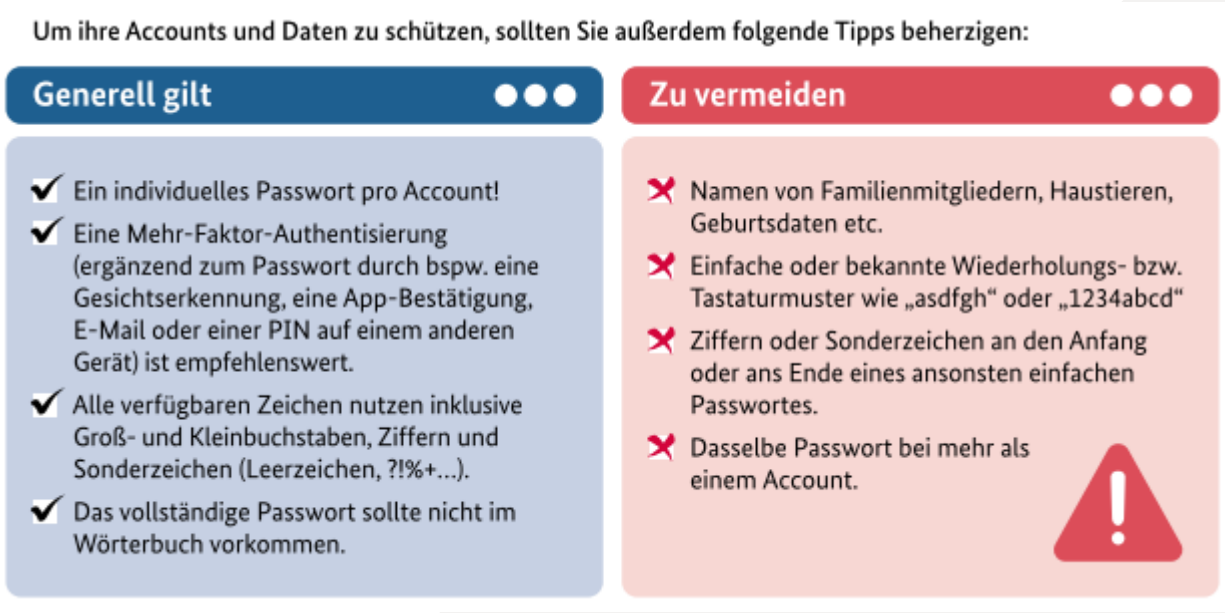
admin

EMPFEHLUNG DES BSI FÜR EIN SICHERES PASSWORT

EWN Entsorgungswerk für Nuklearanlagen

Kurzes dafür komplexes Passwort:

- Acht bis zwölf Zeichen lang
- Besteht aus vier verschiedenen Zeichenarten
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen werden willkürlich aneinandergereiht



Um ihre Accounts und Daten zu schützen, sollten Sie außerdem folgende Tipps beherzigen:

Generell gilt

- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden

- ✗ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✗ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh“ oder „1234abcd“
- ✗ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✗ Dasselbe Passwort bei mehr als einem Account.

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.html

NUTZUNG VON PASSWÖRTERN

EWN Entsorgungswerk für Nuklearanlagen

- Schützen Sie vertraulichen Informationen durch Passwörter.
- Verwenden Sie sichere Passwörter und vermeiden Sie Mehrfachverwendung.
- Geben Sie persönliche Passwörter oder Benutzerkennungen niemals weiter. Auch nicht an Verwandte und Freunde.
- Ändern Sie Ihre Passwörter, wenn sie unberechtigten Dritten bekannt sein könnten.
- Nutzen Sie zum Verwalten Ihrer persönlichen, dienstlichen Passwörter den Passwortmanager „KeePass“
  - auf neuer Hardware vorinstalliert
  - alternativ über Softwareantrag im Self-Service-Portal zu bestellen

PASSWÖRTER ERSTELLEN

EWN Entsorgungswerk für Nuklearanlagen

Eine Methode: Der Merksatz

Ich, als vorbildlicher Mitarbeiter, gelobe die Informationssicherheit zu unterstützen, bis dass…

So könnte ihr Passwort aussehen:

I,avM,gdIzu,bd.

↓

1,avM,gdIzu,6d.

Und so wird es noch vielseitiger.

1,avM,gdIzu,6d.-AMZN	**Für ihr Amazon Konto**
BNK-1,avM,gdIzu,6d.	**Für ihre Online Bank**
1,avM,gdIzu,6d.-PYPL	**Für ihren PayPal Account**

ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)

EWN Entsorgungswerk für Nuklearanlagen

- … oder **Multi-Faktor-Authentifizierung (MFA)** - Identitätsnachweis eines Nutzers durch eine Kombination zweier (oder mehrerer) unterschiedlicher und insbesondere unabhängiger Komponenten; wie beispielsweise Passwort und TAN beim Online-Banking.
- Wichtig ist, dass die Faktoren dabei aus verschiedenen Kategorien stammen.

Wissen (Passwort)

Besitz (Chipkarte)

Biometrie (Fingerabdruck)

Geo-location (Standort)

BEDROHUNGEN UND DEREN FOLGEN

EWN Entsorgungswerk für Nuklearanlagen

Schauen Sie sich dieses Bild an.

Finden Sie alle Alltags-schwachstellen?

Quelle: BSI

BEDROHUNGEN UND DEREN FOLGEN

EWN Entsorgungswerk für Nuklearanlagen

Brandgefahr

Ungeschützte Serverschränke

Offene Fenster

Ungeeignete, ungesicherte Türen

Bildschirm einsehbar

Nutzung privater Geräte

Datensicherungen liegen offen herum

Vertrauliche Informationen In Druckern und Kopierern

Passwort einsehbar

Offenliegende Faxe / Dokumente

Quelle: BSI

MIT DIESEN MAßNAHMEN ERHÖHEN SIE DAS SICHERHEITSNIVEAU!

EWN
Entsorgungswerk für Nuklearanlagen

- Beachten Sie diese Hinweise - auch im Home Office und unterwegs!
- Schließen Sie sensible Unterlagen in Aktenschränke
- Sperren Sie Ihren PC bei Verlassen des Arbeitsplatzes
- Sichern Sie Notebooks vor Diebstahl durch sichere Verwahrung
- Sichern Sie Daten nicht lokal (Desktop), sondern immer auf Netzlaufwerken, SharePoint, etc.
- Nach Besprechungen: Beschriftete Flipchart-Blätter entfernen & Whiteboards reinigen
- Verhindern Sie eine Einsichtnahme durch unberechtigte Dritte, z. B. durch Sichtschutzfolien
- Verhindern Sie das Mithören durch unberechtigte Dritte
- Keine dienstliche Nutzung von privaten Geräten, z. B. Speicherung von dienstl. Telefonnummern
- (Papier-)Dokumente sicher entsorgen

MOBILES ARBEITEN (AUF REISEN UND IM HOMEOFFICE)

EWN Entsorgungswerk für Nuklearanlagen

Für alle Mitarbeitenden gilt die Gesamtbetriebsvereinbarung 01/2022[1)]

„Mobile Arbeit“:

> Daten sind so zu sichern, dass Dritte (bspw. Familienmitglieder, Haustiere, Gäste…) keinen Zugriff erhalten.

> Die Mitnahme papierbasierter Unterlagen (insbesondere VS-NfD, Personal- und Patientenakten, BEM-Unterlagen, Betriebsratsprotokolle) ist nicht gestattet.

> Bestehen Zweifel daran, ob bestimmte Unterlagen mit vertraulichen Daten aus dem Unternehmen an den alternativen Arbeitsort mitgenommen werden dürfen, ist vorher die Zustimmung der Abteilungsleitung einzuholen.

> Für eine sachgemäße Vernichtung von Unterlagen ist Sorge zu tragen. Verwenden Sie ausschließlich Shredder oder bereit gestellte Container im Unternehmen.

1) https://intranet.intern/personal/betriebsvereinbarungen

DATEN UND DATENTRÄGER

EWN Entsorgungswerk für Nuklearanlagen

Für alle Mitarbeitenden gilt OHB[1)] Teil III Kapitel 7.1
„Organisation des Datenverarbeitungsprozesses“:

- Unternehmenseigene Daten dürfen nicht auf privaten Computern bearbeitet oder gespeichert werden.
- Private Daten dürfen nicht auf Unternehmenseigenen Computern bearbeitet oder gespeichert werden.
- Private Technik ist nicht in der EWN einzusetzen
  - Ausnahmen sind schriftlich durch die zuständige Abteilungsleitung und die IT-Abteilung zu regeln
- Datenträger (USB-Sticks…) sind einer Virenprüfung zu unterziehen.

LÖSCHEN – VERNICHTEN – VERLIEREN

EWN Entsorgungswerk für Nuklearanlagen

- Entsorgen Sie dienstliche Dokumente ausschließlich in den dafür vorgesehenen Sammelbehältern oder schreddern Sie diese mit geeigneten Aktenvernichtern.
- Datenträger (USB-Sticks, Festplatten etc.) über KDI entsorgen.
- Leeren Sie nach dem Löschen von Dateien auch den Windows-Papierkorb.
- Melden Sie den unbeabsichtigten Verlust dienstlichen Daten unverzüglich Ihrem Vorgesetzten und / oder der betrieblichen DSB, z. B. wenn Sie Dokumente oder mobile Geräte oder Speicher wie USB-Sticks verlieren!
- Machen Sie sich mit den spezifischen Regelungen zu Datenschutz und IT-Sicherheit im Unternehmen und in ihrem Fachbereich vertraut!

VERSCHLÜSSELUNG

EWN Entsorgungswerk für Nuklearanlagen

> Nutzen Sie die gängigen Verschlüsselungsmöglichkeiten[1] in der EWN:
  - Cryptshare (E-Mail)
  - VeraCrypt (längerfristige Verschlüsselung besonders sensibler Daten)
  - 7-Zip (einmalige Verschlüsselung von Dateien)
  - **Nicht** geeignet ist der Kennwortschutz von MS-Office.
  - Die Anleitungen finden Sie im Intranet[2]

> E-Mails und Telefaxe sind nicht sicherer als Postkarten! Versenden Sie vertrauliche Daten daher NICHT per Fax oder als unverschlüsselte E-Mail.
  - Kontrollieren Sie bei E-Mails die Empfängerliste, insbesondere bei der Nutzung der „Allen-Antworten-Funktion“.

1) Achtung: verschlüsselte Daten können NICHT wiederhergestellt werden, wenn das Passwort verloren geht oder die Datei beschädigt wird.
2) https://intranet.intern/informationsshytechnik/anleitungen

PRAXISTIPPS FÜR DIE PRIVATE NUTZUNG

EWN Entsorgungswerk für Nuklearanlagen

Ein Online-Dienst, der Dateien und Webseiten mit über 70 verschiedenen Antivirenprogrammen und Malwarescannern analysiert:
Virustotal.com

Have I been pwned:

https://haveibeenpwned.com/

DFN Terminplaner für Terminabstimmungen:
https://intranet.intern/terminplaner

Lassen Sie keine beruflichen Dateien mit personenbezogenen Daten überprüfen. Die Datenverarbeitung findet außerhalb der EU statt.

FAZIT / AUSBLICK

EWN Entsorgungswerk für Nuklearanlagen

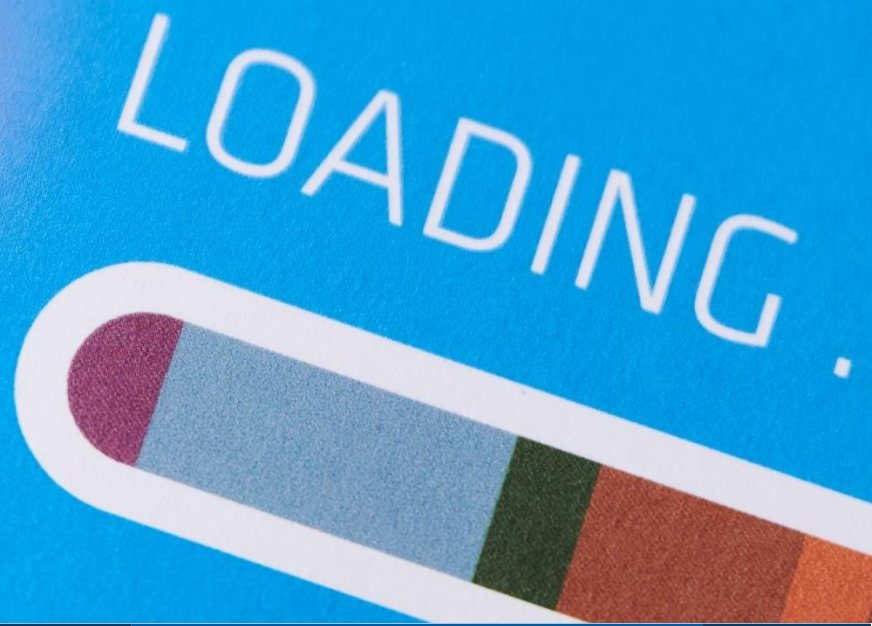
- Jeder Beschäftigte beeinflusst das Sicherheitsniveau durch sein tägliches Handeln – positiv wie negativ.
- Informationssicherheit ist nicht nur eine Aufgabe der Leitung und des Informationssicherheitsteams, sondern alle Beschäftigten sind hierfür in Ihrem Wirkungsbereich verantwortlich. Ohne Ihre Mitwirkung wird eine Institution die gesetzten Sicherheitsziele verfehlen.
- Kontaktieren Sie Ihren Informationssicherheitsbeauftragten immer, wenn Sie
  - eine Schwachstelle oder akute Bedrohung vermuten oder feststellen
  - Fragen zur Informationssicherheit haben

12/18/2024

EWN Entsorgungswerk für Nuklearanlagen

adesso

VIELEN DANK!



Mit Unterstützung durch:
adesso SE
Adessoplatz 1
44269 Dortmund
T +49 231 7000-7000
F +49 231 7000-1000
www.adesso.de