Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Cyberangriffe auf die Komponente Mensch im Energiesystem

Stefan Sütterlin
Fakultät Informatik
Hochschule Albstadt-Sigmaringen
suetterlin@hs-albsig.de

Stuttgart, 24.07.2025

Welche Rolle spielt der Faktor Mensch?

Wie wird damit umgegangen?

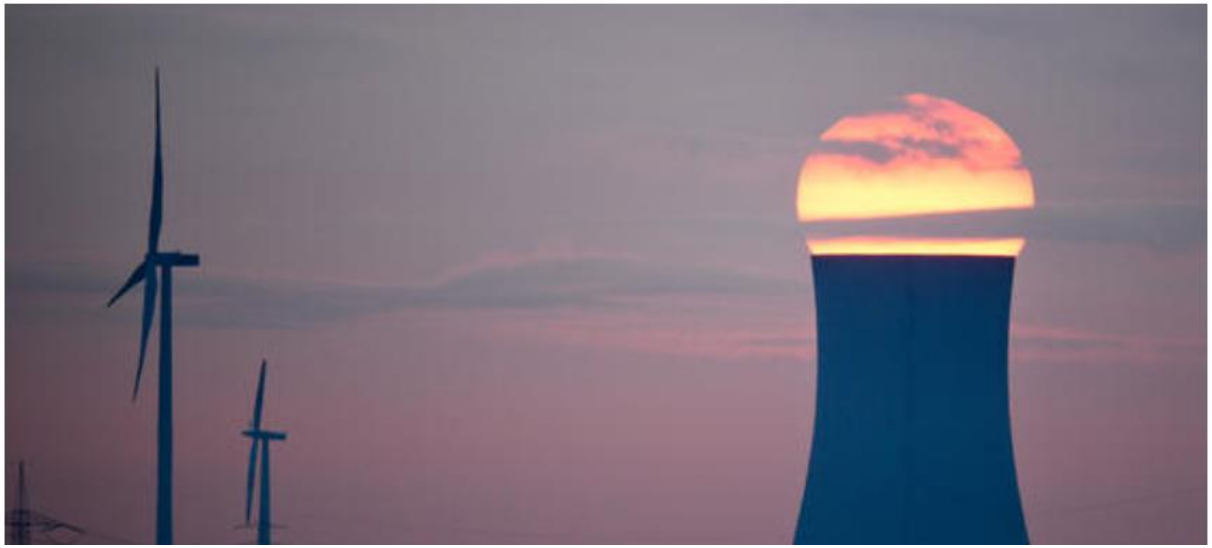
Was sind die Konsequenzen?

SICHERHEITSEXPERTEN WARNEN

11.09.2017, 07:33 Uhr

Sabotage geplant: Hacker wollen Kraftwerke ausschalten

Cyberkriminelle spionieren derzeit Kraftwerke in Europa und Nordamerika aus, um sie später gezielt sabotieren zu können. Davor warnt die US-Sicherheitssoftwarefirma Symantec. Sie hat nach eigenen Angaben konkrete Hinweise für entsprechende Pläne. Auch Kraftwerke in Deutschland seien ins Visier der Hacker geraten.



Digitalisierung und Dezentralisierung, IT/OT-Interkonnektivität

Neue Technologien => Angriffsfläche

- Smart Grids
- Cloud-Plattformen
- IoT-Sensorik
- Smart Meter

+ Altanlagen mit hohem **Nachholbedarf** bei Segmentierung, Härtung und Überwachung.

Unvollständige Beispielliste

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Jahr	Organisation	Angriffsart	Folgen
2022	Rheinenergie	Phishing / Malware	IT-Systeme ausgefallen
2022	Entega / GISA	Ransomware über Dienstleister	Kommunikation gestört
2021–2023	E.ON	Phishing-Kampagnen	Angriffe abgewehrt
2021	Stadtwerke Wismar	Malware	Betrieb eingeschränkt
2018–2021	TRISIS-Fall	ICS-Malware	Sicherheitssteuerung gefährdet
2023	dena	Ransomware (BlackCat)	Server abgeschaltet, Datenleak
2024	PSI Software	Unbekannt / gezielter Angriff	Schnittstellen getrennt
2023	Stadtwerke Karlsruhe	Schadsoftware	Sicherheitsmaßnahmen verstärkt
2024	Tibber	Datendiebstahl	50.000 Kundendaten betroffen

Handelsblatt

Energieversorger

Hackerangriff trifft Enercity härter als gedacht: Zahlungsverkehr eingeschränkt

Einer von Deutschlands größten Energieversorgern hat mit den Folgen eines Cyberangriffs zu kämpfen. Davon betroffen sind auch der Mail- und Telefonverkehr der Firma aus Hannover.

Catiana Krapp und Claudia Scholz
08.11.2022 - 09:05 Uhr

Ransomware bei Energieversorger

"Erstaunlich, in was für einer Gefahr sich Unternehmen befinden"

4. Oktober 2023, 15:23 Uhr

Süddeutsche Zeitung

Konzernchefin Susanna Zapreva: "Ich gehörte auch zu den Menschen, die dachten, so was passiert uns nicht so einfach."
(Foto: Christian Kerber)

„Ich gehöre auch zu den Menschen, die dachten, so was passiert uns nicht so einfach.“

„Probability Weighting“

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Wie wir mit sehr geringen Wahrscheinlichkeiten umgehen, hängt davon ab, wie wir sie bewerten.

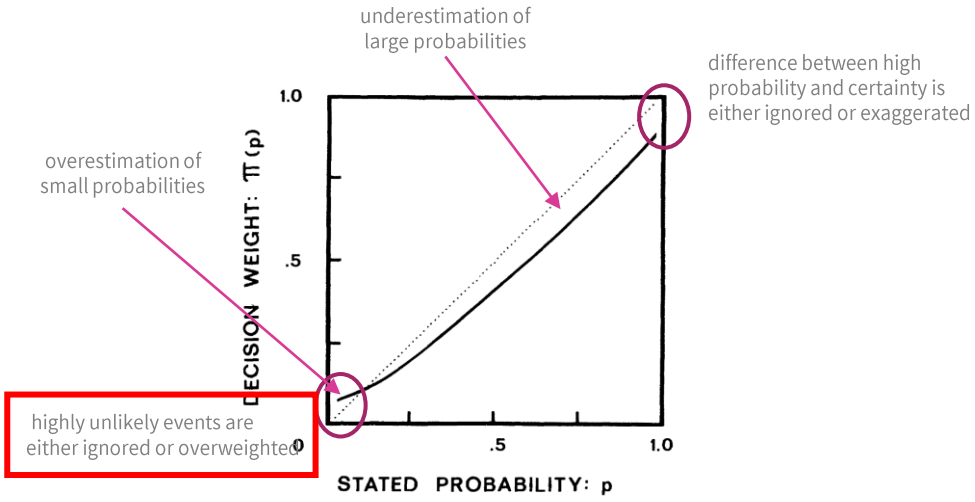


FIGURE 4.—A hypothetical weighting function.

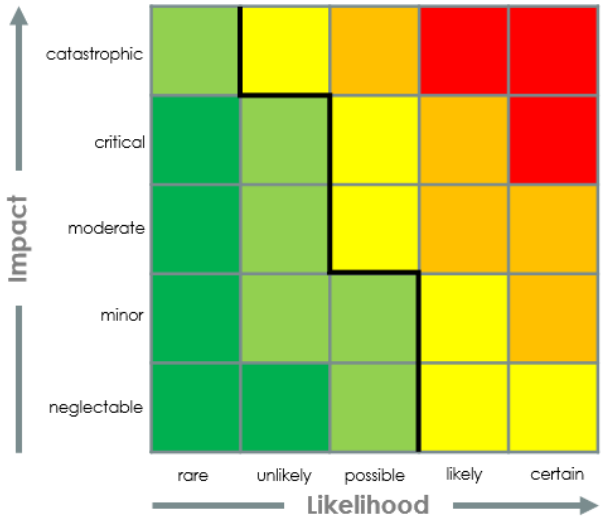
Kahneman, Tversky (1979)

„Investition“ oder „Ausgabe“?

Um zu verstehen, dass ich investiere, muss ich wissen in was ich investieren soll.

Risiko = Eintrittswahrscheinlichkeit x Schadensausmaß (ISO 31000)

$$E(Risiko) = \sum_i P_i \times S_i$$



Wahrgenomme Risiken

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Archiv

Kommentar zum Ahrtal

Ein Wiederaufbau ohne Konzept

135 Menschen starben durch die Flutkatastrophe vor zwei Jahren allein im Ahrtal. 9000 Gebäude wurden auf dem 40 Kilometer langen Flussabschnitt zerstört. Fast alle werden an alter Stelle wiederaufgebaut – das sei gewagt, kommentiert Anke Petermann.

Ein Kommentar von Anke Petermann | 15.07.2023

Wiederaufbau an der Ahr, zwei Jahre nach der Flutkatastrophe im Juli 2021. Viele Gebäude werden am gleichen Ort wieder errichtet. Die Gefahr einer erneuten Überflutung bleibt. (imago / Marc John)

Die Ahr hat ihr Potenzial mit der Flut vom Sommer 2021 noch nicht ausgeschöpft. Dieses Urteil des Bonner Hochwasserexperten Thomas Roggenkamp vor dem Untersuchungsausschuss Flutkatastrophe des Mainzer Landtags schockiert. Man hätte es den Entscheidungsträgern in Bund und Ländern einhämmern sollen, bevor sie an der Fördersystematik des 30 Milliarden Euro schweren Aufbauhilfefonds strickten.

Denn diese führt mit dazu, dass 99 Prozent aller flutverwüsteten Gebäude in Rheinland-Pfalz und Nordrhein-Westfalen an alter Stelle flussnah wiederaufgebaut werden. Teils, weil Betroffene den privaten Raum in ihrer Heimat schnell zurückhaben wollen – verständlich angesichts der großen Belastungen. Teils aber auch, weil Geschädigte sich gezwungen sehen, trotz unguter Gefühle am selben risikoreichen Ort wiederaufzubauen.

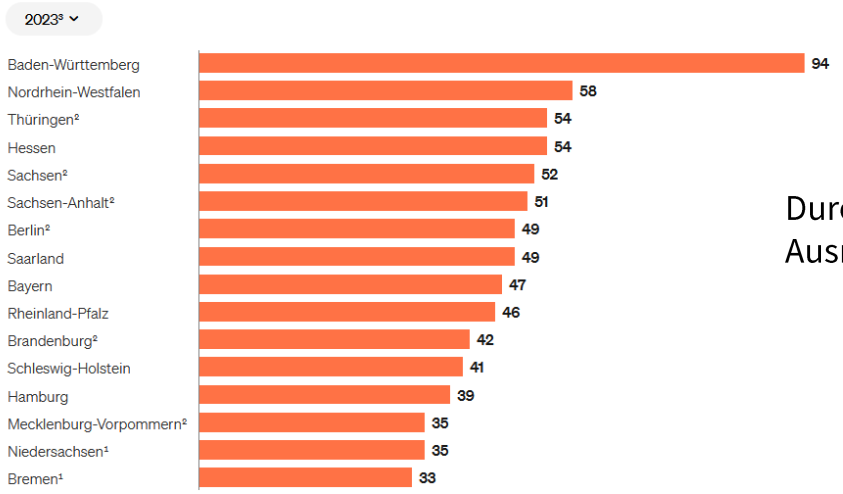
https://www.deutschlandfunk.de/ahrtal-flutkatastrophe-100.html

Zum Thema Einsicht

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Wohngebäudeversicherung – weitere Naturgefahren-(Elementar-)volldeckung, Versicherungsdichte pro Bundesland in % (bezogen auf Wohngebäude-Feuer)

ohne reine Starkregenverträge und mit sogenannten Altverträgen der ehemaligen Deutschen Versicherungs-AG;
in Prozent



Gesamtverband der Versicherer (2024)

Versicherungspflicht in Baden –Württemberg bis 1993.

Durchschnittliche jährliche Kosten zwischen €50 and €300, in Ausnahmefällen bis zu €1000.

Diskrepanz zwischen Anspruch und faktischer Anforderung

L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

27.12.2022 EN Official Journal of the European Union L 333/95

(77) Responsibility for ensuring the security of network and information system lies, to a great extent, with essential and important entities. A culture of risk management, involving risk assessments and the implementation of cybersecurity risk-management measures appropriate to the risks faced, should be promoted and developed.

27.12.2022 DE Amtsblatt der Europäischen Union L 333/95

(77) Die Verantwortung für die Gewährleistung der Sicherheit von Netz- und Informationssystemen liegt in erheblichem Maße bei den wesentlichen und wichtigen Einrichtungen. Es sollte eine Risikomanagementkultur gefördert und entwickelt werden, die unter anderem die Risikobewertung und die Anwendung von Risikomanagement-maßnahmen im Bereich der Cybersicherheit, die den jeweiligen Risiken angemessen sind, umfassen sollte.

Lösung: Regulatorik (?)

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

NIS2-Verantwortlichkeiten und Konsequenzen für das Management

Schulung & Sensibilisierung
Geschäftsleitungen müssen regelmäßige Schulungen zu Cyberrisiken und -abwehr erhalten.

Sanktionen & Strafen
Hohe Bußgelder bei Verstößen – auch persönliche Haftung von Führungskräften möglich.

Aufsicht & Rechenschaft
Pflicht zur Einführung eines internen Kontrollsystems zur Überwachung der NIS-2-Compliance.

Aufsichtsbehörden
Nationale Behörden prüfen Pflichterfüllung und können persönliche Strafen verhängen.

Was also tun?

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

1. Schulung

Bundesamt
für Sicherheit in der
Informationstechnik

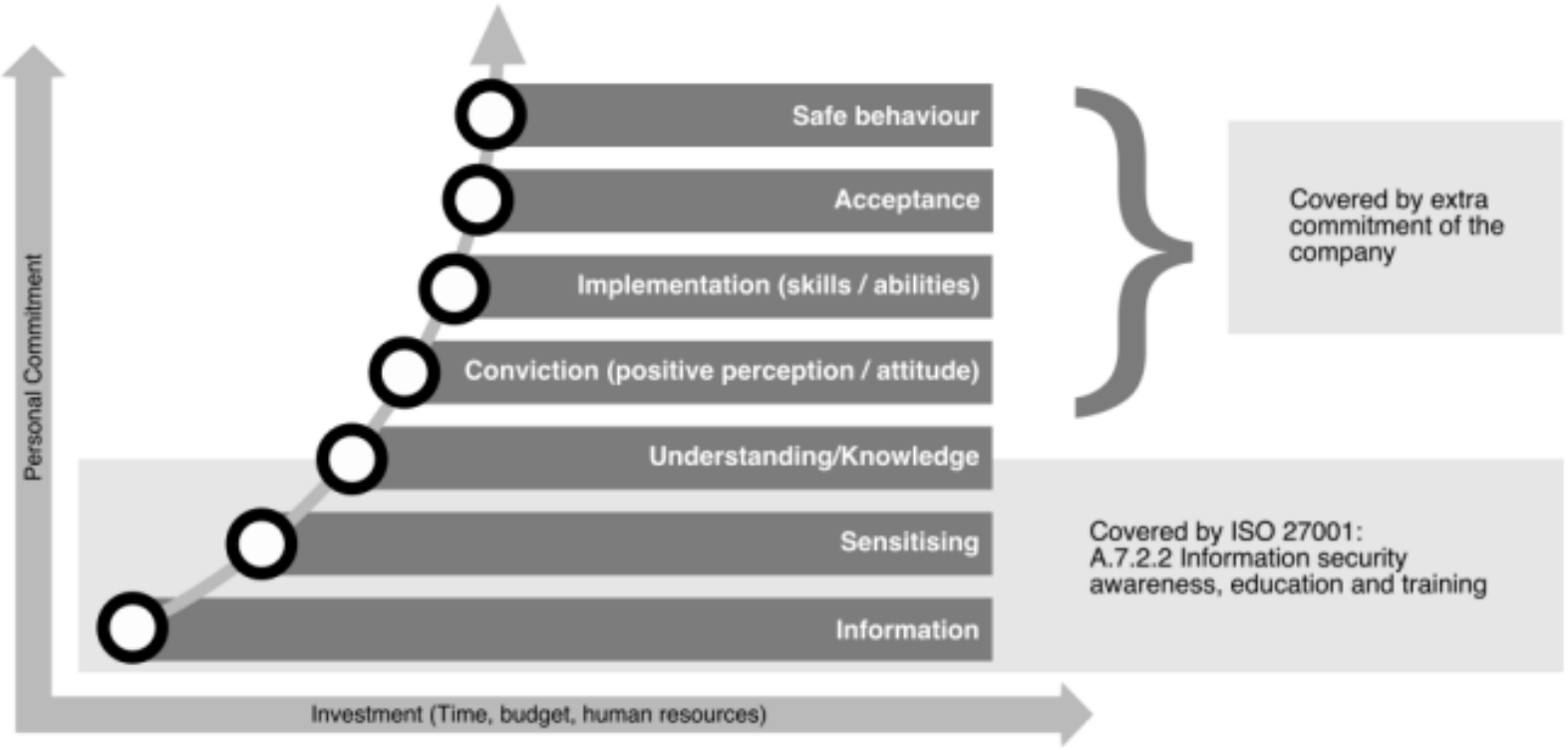
Deutschland
Digital•Sicher•BSI•

Positionspapier: Cybersicherheit im Energiesektor Deutschlands

Kapitel 6: Notwendige Maßnahmen

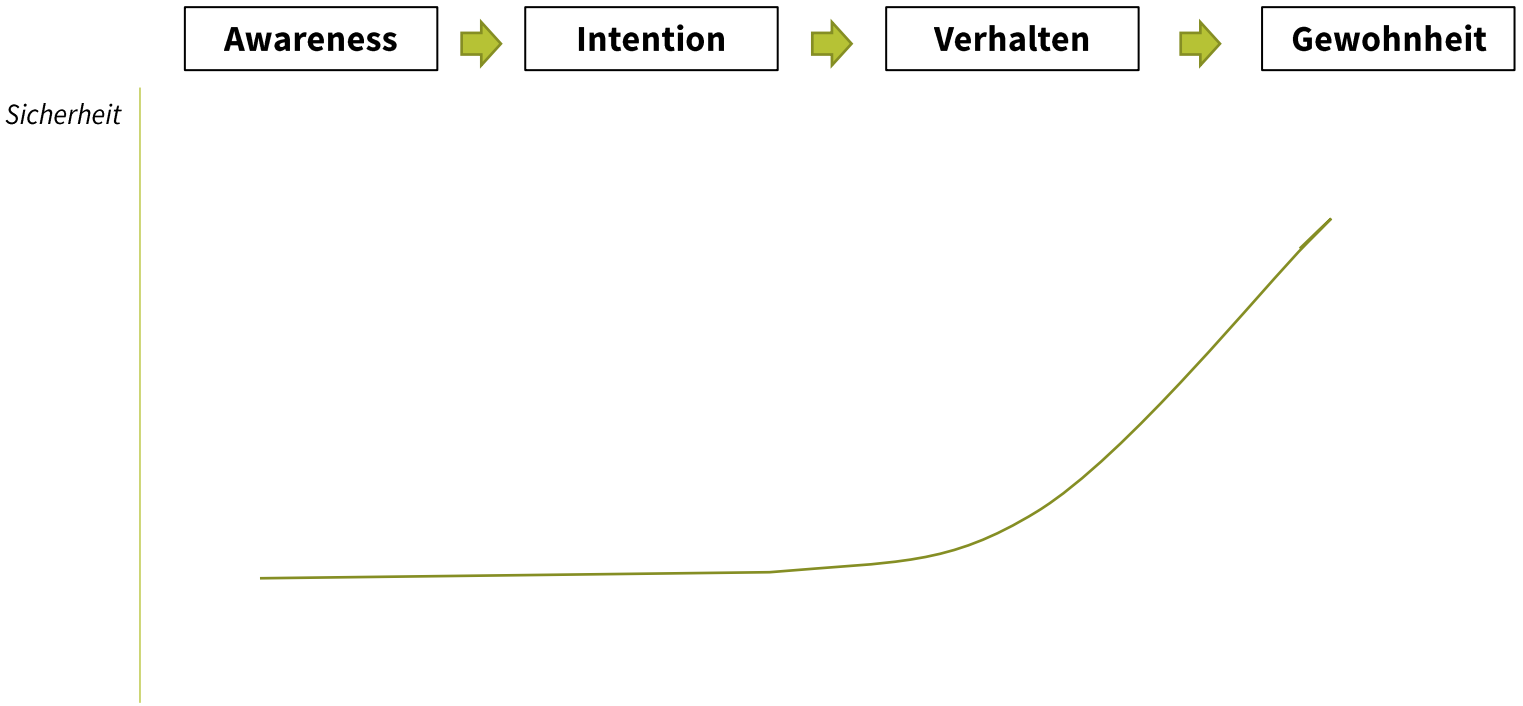
„Schulung von Personal entlang der gesamten Wertschöpfungskette im Umgang mit Cybergefahren.“ (S. 3)

Geringstmögliche Nachfrage trifft auf fragwürdige Qualität



(Roer & Carpenter, 2023)

'It would be easy to give the public information and hope that they change behaviour but we all know that doesn't work very satisfactorily. Otherwise none of us would be obese, none of us would smoke and none of us would drive like lunatics'
(Potter et al., 2007)


Awareness
Intention
Verhalten
Gewohnheit
Sicherheit

… Gewohnheiten größerer Gruppen von Menschen zu ändern, war nicht Teil Ihrer IT-Ausbildung…?

… sie ziehen es vor, sich auf technische Maßnahmen zu konzentrieren…?

SPECIAL SECTION: 2017 Human Factors Prize Winner

Hacking the Human: The Prevalence Paradox in Cybersecurity

Ben D. Sawyer, Massachusetts Institute of Technology, Cambridge, and **Peter A. Hancock**, University of Central Florida, Orlando

Objective: This work assesses the efficacy of the "prevalence effect" as a form of cyberattack in human-automation teaming, using an email task.

Background: Under the prevalence effect, rare signals are more difficult to detect, even when taking into account their proportionally low occurrence. This decline represents diminished human capability to both detect and respond. As signal probability (SP) approaches zero, accuracy exhibits logarithmic decay. Cybersecurity, a context in which the environment is entirely artificial, provides an opportunity to manufacture conditions enhancing or degrading human performance, such as prevalence effects. Email cybersecurity prevalence effects have not previously been demonstrated, nor intentionally manipulated.

Method: The Email Testbed (ET) provides a simulation of a clerical email work involving messages containing sensitive personal information. Using the ET, participants were presented with 300 email interactions and received cyberattacks at rates of either 1%, 5%, or 20%.

Results: Results demonstrated the existence and power of prevalence effects in email cybersecurity. Attacks delivered at a rate of 1% were significantly more likely to succeed, and the overall pattern of accuracy across declining SP exhibited logarithmic decay.

Application: These findings suggest a "prevalence paradox" within human-machine teams. As automation reduces attack SP, the human operator becomes increasingly likely to fail in detecting and reporting attacks that remain. In the cyber realm, the potential to artificially inflict this state on adversaries, hacking the human operator rather than algorithmic defense, is considered. Specific and general information security design countermeasures are offered.

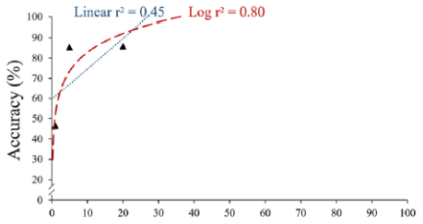


Figure 3. The logarithmic fit for these data proves superior to linear fit, suggesting that the pattern found is one of logarithmic decay of accuracy as signal probability (SP) approaches zero. This is consistent with patterns seen in past research of the prevalence effect (Mitroff & Biggs, 2014).

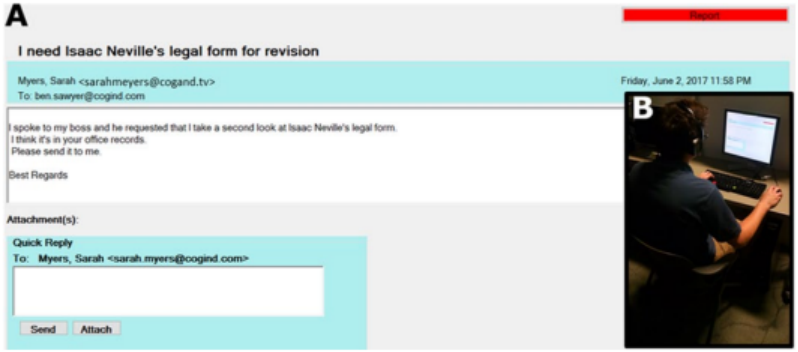
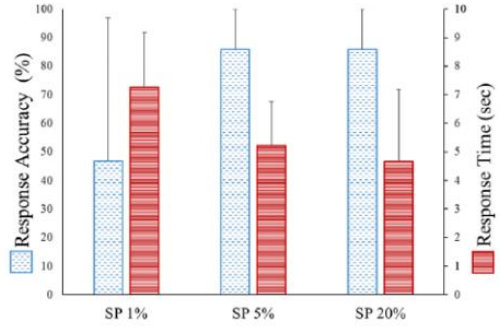


Figure 1. (A) The Email Testbed (ET) was designed to simulate interaction in common online commercial webmail interfaces. Participants received emails asking them to upload or download secure documents. Cyberattack emails had multiple cues as to their nature—in this phishing email, for example, the inbound address, ending in ".tv," and the body of the email, lacking a signature. Should a participant improperly upload and send a document, a miss would be recorded. Should the participant click on the red "Report" button, a correct detection would be recorded. Attack emails were received at rates of 1%, 5%, or 20%. (B) Each participant addressed 300 such emails. Headphones playing white noise were used to minimize distraction by ambient sound and to deliver instructions at the end.



Was also tun?

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

2. Austausch

Offenheit im Umgang

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

dena

Themen der dena | Projekte der dena | Infocenter Artikel, Events, Presse | Über die dena Mission, Organisation, Jobs

Start > Infocenter > Hackergruppe veröffentlicht gestohlene Daten

09.02.24

Hackergruppe veröffentlicht gestohlene Daten

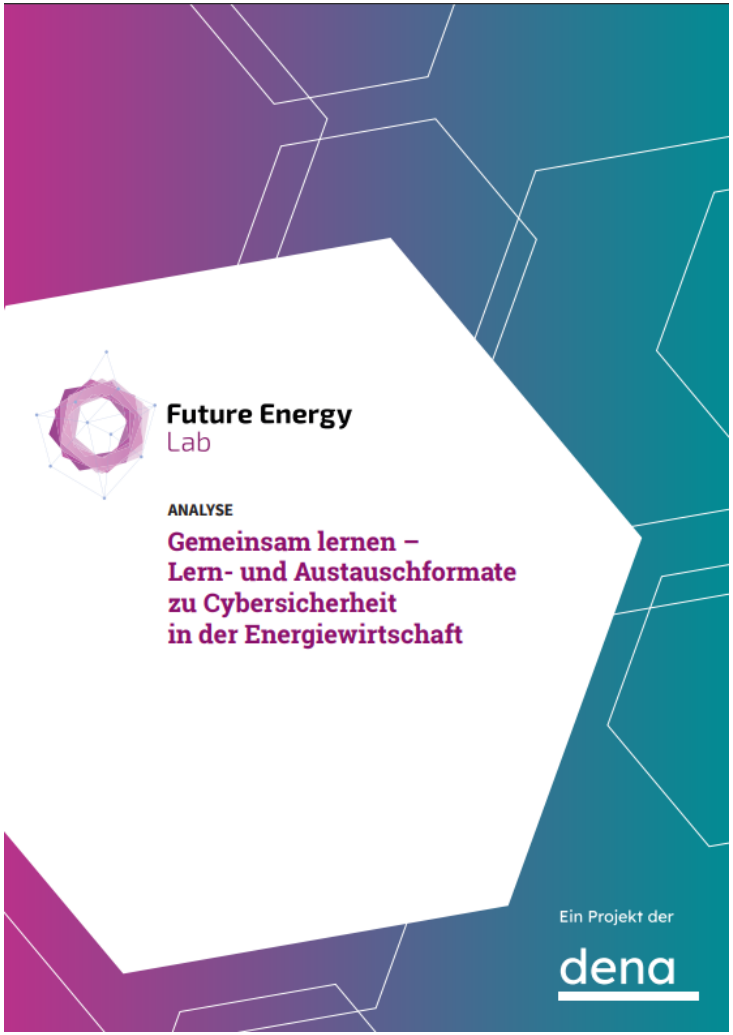
Berlin, 09. Februar 2024. Nach dem Cyberangriff auf die Deutsche Energie-Agentur (dena) am 13.11.2023 hat die Hackergruppe Lockbit von der dena gestohlene Daten im Darknet veröffentlicht. Nach einer ersten Prüfung dieser gestohlenen Datensätze hat die dena die von der Veröffentlichung Betroffenen dazu informiert, welche ihrer Daten betroffen sein können. Mit dem Bundesministerium für Wirtschaft und Klimaschutz (BMWK) als Vertreterin der Gesellschafter und weiteren staatlichen Stellen steht die dena in engem Kontakt. Zur Analyse des Vorfalls und zum Aufbau von Schutzmechanismen hat die dena verschiedene Dienstleister hinzugezogen.

Zum Hintergrund und Hergang: Am 13.11.2023 wurde die dena Opfer einer Ransomware-Attacke. Zur Gefahrenabwehr wurden sämtliche Server der dena umgehend heruntergefahren. Die Öffentlichkeit wurde am 14.11.2023 über den Angriff via Pressemitteilung und über die dena-Website informiert. Zuvor wurden die staatlichen Stellen informiert und Strafanzeige gestellt. Sobald die dena wieder Zugang zu ihren Kontaktdatenbanken hatte und durch Einrichten einer neuen E-Mail-Lösung in der Lage war, wieder E-Mails zu versenden, wurden alle Geschäftskontakte der dena via E-Mail und über die Website zu dem Daten-Diebstahl informiert.

Zum Angriff auf die dena hat sich die Hackergruppe BlackCat bekannt. BlackCat geht nach einem immer gleichen Muster vor und droht Daten zu veröffentlichen, wenn ihren Lösegeldforderungen nicht nachgekommen wird. Nach rund drei Wochen hatte die Gruppe auf ihrer Website die dena als erpresstes Unternehmen gelistet und angekündigt, Daten zu veröffentlichen. Wenig später sind die Websites von BlackCat nicht mehr erreichbar gewesen. Eine internationale Ermittlergruppe, unter Führung US-amerikanischer Behörden, hatte die Hackergruppe Anfang Dezember lahmgelegt. Stattdessen trat kurz darauf eine andere Hackergruppe (Lockbit) mit der Ankündigung auf, sie sei im Besitz der gestohlenen dena-Daten und würde sie veröffentlichen. Das gestellte Ultimatum verlief zunächst ohne weitere Aktivitäten.

Gemeinsam lernen

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University



Inhalt

https://www.dena.de/infocenter/gemeinsam-lernen/ -

Fazit

Welche Rolle spielt der Faktor Mensch?

- Eine entscheidende in der Mehrzahl der Angriffe, die durch menschliches Fehlverhalten zustande kamen oder begünstigt wurden.
- Eine entscheidende im Sinne eines enormen Risikoreduktionspotenzials.

Wie wird damit umgegangen?

- Verzerrte Risikowahrnehmung bei low-probability-high-impact Ereignissen.
- Prävention als Ausgabe anstatt ROI-Perspektive, mangelnde KPIs.
- Too little, too late.

Was sind die Konsequenzen?

- Unnötig hohes Risiko.
- Notwendigkeit, substanziell in Schulungsmaßnahmen zu investieren als ergänzende (nicht ersetzende) Risikomanagementmaßnahme.
- Notwendigkeit von Qualitätssicherungsmaßnahmen und eingehender Prüfung von Angeboten angesichts fragwürdiger externer Beratungsleistungen.

Was wir als staatliche Hochschule bieten

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Neutrale Einschätzungen Ihrer Bedürfnisse.

Vergleich von Angeboten externer Dienstleistungen.

Tipps für kritische Nachfragen und Kriterien zur Beurteilung kommerzieller Angebote.

- Individualisierbarkeit
- Nachhaltigkeit
- Evidenzbasierte Entscheidungen und validierte Lernformate
- Verhaltensfokusiert
- Sicherheitskultur-Konzept
- …

“And you know cyber is becoming so big today. It’s becoming something that a number of years ago, a short number of years ago, wasn’t even a word. And now the cyber is so big, and you know you look at what they’re doing with the internet.

But cyber has been very, very important and it’s becoming more and more important as you look and a lot of it does have to do with ***ideology and psychology and a lot of other things****. You know, we’re in a very different world than we were in 20 years ago, 30 years ago.”*

Donald J. Trump, President of the United States.
Sept. 7, 2016

Vielen Dank!

Bei Fragen, Rückmeldungen oder sonstigen Wünschen, melden Sie sich gern zu einem unverbindlichen (und natürlich kostenlosen) Erfahrungsaustausch!

suetterlin@hs-albsig.de

Update: Plattner fordert Schutz der Energieversorgung

Versteckte Kommunikationsmodule in Solarwechselrichtern aus China

16.05.2025 Aktualisiert am 28.05.2025 · Von **Melanie Staudacher** · 4 min Lesedauer ·

US-Energiebehörden äußerten Sicherheitsbedenken hinsichtlich chinesischer Solarwechselrichter, nachdem in einigen Geräten nicht dokumentierte Kommunikationsmodule entdeckt wurden. Diese könnten eine Umgehung von Firewalls ermöglichen und Fernzugriffe auf das Stromnetz erlauben.