Cyber Awareness bei der MVV Energie AG

Gerhard Voelkner, Security Governance

Mannheim, 28.01.2025

Wir begeistern mit Energie.

Gerhard Voelkner

Dipl. ing. phys.

- Zunächst leitende Tätigkeit im internationalen Projektmanagement, anschließend Positionswechsel in die Informationssicherheit
- Seit vielen Jahren im Bereich der IT-Security tätig, davon 5 Jahre in den Landesministerien Mecklenburg-Vorpommern als Security-Manager
- Seit 2017 bei der MVV Energy AG in verantwortlicher Position für diverse Aufgabenbereiche im Bereich Security Governance
- Maßgebliche Beteiligung am Schutz des Unternehmens vor Cyber-Bedrohungen
- Vor 5 Jahren Einführung einer **interaktiven konzernweiten Awarenessplattform**

Kurze Vorstellung des Unternehmens

MVV Energie AG

Wir begeistern mit Energie

Mit über 6.600 Mitarbeitenden sowie einem Jahresumsatz von rund 7,2 Milliarden Euro im Geschäftsjahr 2024 ist MVV eines der **führenden Energieunternehmen in Deutschland.** Im Zentrum unseres Handelns steht die **zuverlässige, wirtschaftliche und umweltfreundliche Energieversorgung** unserer Kunden aus Industrie, Gewerbe und Privathaushalten.

Wir sind Vorreiter bei der Energiewende und haben uns mit unserem Mannheimer Modell einem strategischen Weg verpflichtet, mit dem wir als eines der ersten Energieunternehmen Deutschlands bis 2035 #klimapositiv werden.

MVV Energie AG
Wir auf einen Blick

128
Vollkonsolidierte **Gesellschaften**

Vertreten u. a. in

Deutschland
und
Großbritannien

Größte **Standorte**

Mannheim
Kiel **Wörrstadt**
Offenbach
Plymouth
Dundee

6.649
Beschäftigte (zum 30.9.2024)

MVV Energie AG
Unsere Geschäftsfelder

Kundenlösungen

- Privat- und Gewerbekunden
- Geschäftskunden
- Commodity Services

Neue Energien

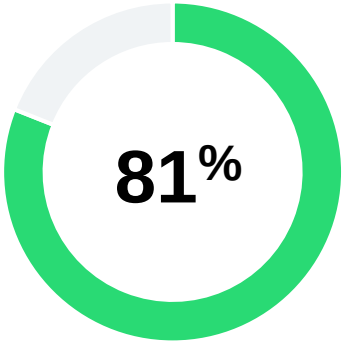
- Umwelt Deutschland
- Umwelt UK
- Wind und PV

Erzeugung und Infrastruktur

- Erzeugung
- Netze

Die aktuellen Angriffsvektoren

Bedrohungslage und Angriffstatistiken



aller Sicherheitsbeauftragten sind der Meinung, dass die **Cyber-Bedrohungslage** in den letzten fünf Jahren nie angespannter war als heute, und ...

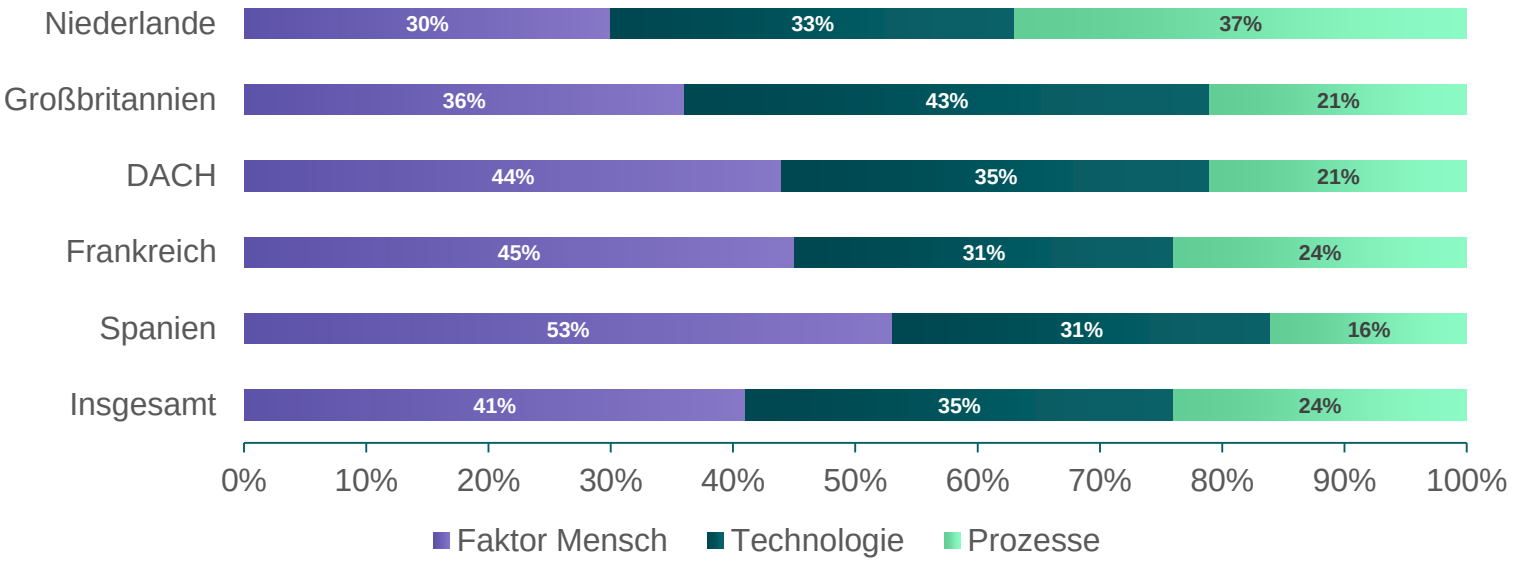
... weniger als ein Drittel glauben, dass sich die Situation in den nächsten 12 Monaten **verbessern** werde.

Die Top 4 der erfolgreichsten Cyber-Angriffstaktiken

1. Phishing
2. Malware
3. DDoS
4. Ransomware

Der Faktor „Mensch“

Frage: Wo wird Ihrer Meinung nach ein Cyberangriff, der erhebliche negative Auswirkungen auf Ihr Unternehmen hätte, am ehesten seinen Ursprung haben?



Verizon (2024). 2024 Data Breach Investigations Report

Die Awarenessplattform im Wandel

- von der Historie in die Gegenwart -

Die historische Welt – ein Beispiel

Wir begeistern mit Energie

Vertraulichkeit

Die **Vertraulichkeit** von Daten und Informationen ist gegeben, wenn ausschließlich befugte Personen auf diese zugreifen können.

Verfügbarkeit

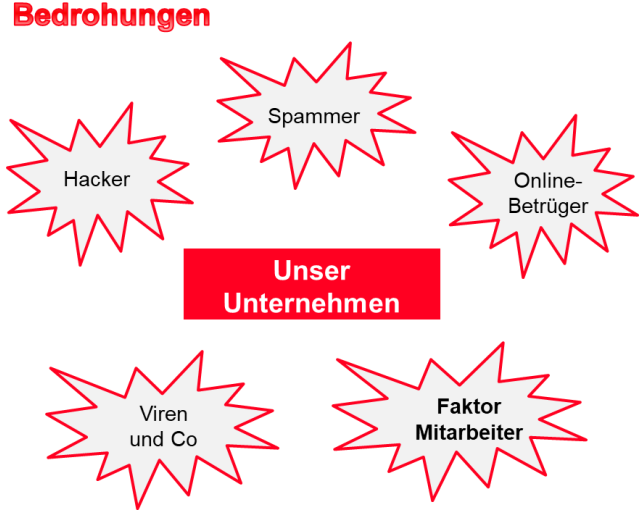
Die **Verfügbarkeit** von IT-Systemen, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Nutzern stets wie vereinbart zur Verfügung stehen.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Verlässlichkeit, Unversehrtheit) von Daten und der korrekten Funktionsweise von IT-Systemen. Anders gesagt: Daten dürfen nicht unbemerkt verändert werden und alle Änderungen müssen nachvollziehbar sein.

Authentizität

Mit dem Begriff **Authentizität** wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.



Welche Auswirkungen können Bedrohungen wie Hacker auf das Unternehmen haben?

- [x] Das Unternehmen kann wirtschaftliche Schäden erleiden.
- [ ] Die Auswirkungen sind nicht bedrohlich, da es genügend Schutzprogramme gibt.
- [x] Es kann ein Imageverlust für das Unternehmen entstehen.
- [x] Kunden können über einen Verlust von personenbezogenen Daten verärgert sein.

Das Umdenken
Beweggründe und Ziele

- Traditionelle Trainingsmethoden erreichten nicht die angestrebten Ziele
  - Statische Inhalte über eine lange Zeitperiode
  - Einfachste und unflexible Möglichkeiten der Informationsdarstellung und –aufarbeitung
  - Wenig eingängige Methoden und mangelnde nachhaltige Informationsaufnahme durch den Mitarbeiter (kein nachhaltiger und bewusster Lerneffekt ▸ keine effektive Umsetzbarkeit der Sicherheitsprinzipien)
- Einführung einer interaktiven und dynamischen Darstellung
  - Inhalte vermitteln, die Bewusstsein unmittelbar erreichen und langfristig zugänglich bleiben
  - Kurze Lerninhalte, modernes Design, Gamification-Elemente

Lösungsansatz

- Etablierung und Berücksichtigung psychologischer und pädagogischer Aspekte ▸ Ausrichtung des ganzheitlichen Blickes auf das menschliche Verhalten und seine Kognition
- Einkauf psychologischer und pädagogischer Ansätze in der Vermittlung von Lerninhalten
- Testlauf mit 3 Produkten und Bewertung durch den Mitarbeiter
- Entscheidung fiel auf ein Produkt, das den Anforderungen des deutschen und europäischen Marktes am stärksten gerecht wird (SoSafe)
- Ergebnis: 4,8 Punkte von 5 möglichen Punkten in der Zufriedenheit und Anwendbarkeit der neuen Plattform erreicht.
- Konzernweite Einführung des Produktes im Jahre 2020
- Einblick in die Online Plattform "Live"

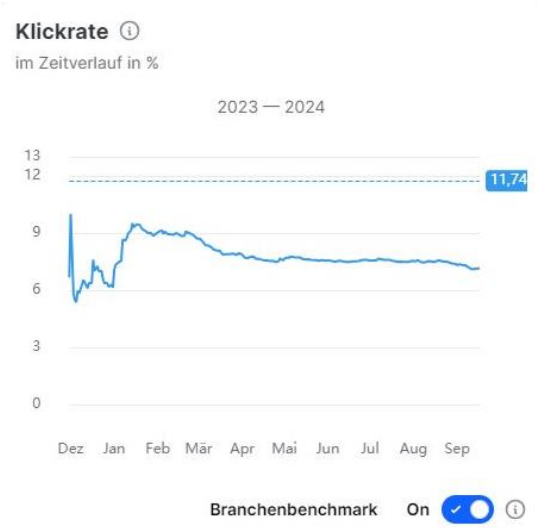
Die Nennung des Produktes dient ausdrücklich **nicht** zu Werbezwecken.

Phishing Simulation
Praxisnahes lernen

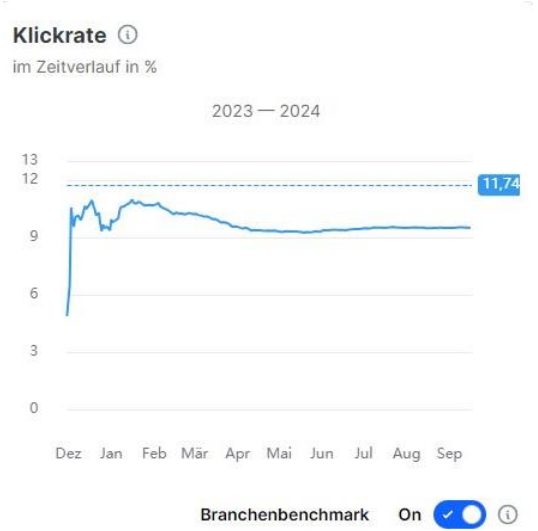
- Theoretisches Wissen in der Praxis umsetzen
  - Realistische Szenarien mit zunehmendem Schwierigkeitsgrad
  - Erlerntes anwenden und festigen
  - Echte Angriffe schnell erkennen und richtig reagieren
  - Stärkung der Unternehmens-Resilienz gegenüber Cyber-Attacken
- Zusammenhänge zwischen Schulung, Klickraten und persönliches Setting
  - 3 Jahre freiwillige Schulungen vs. verpflichtende Schulungen
  - Klickraten und Interaktion werden gemessen
  - Das persönliche Setting spielt eine große Rolle

Phishing Simulation
verpflichtende vs. freiwillige Schulungen

Verpflichtende Schulungen



Freiwillige Schulungen



Lessons Learned

Das sollte unbedingt beachtet werden

- Frühe Einbindung des Betriebsrates bzw. Personalrates
- Ggf. eine Betriebsvereinbarung abschließen, wenn Schulungen verpflichtend sind
- Auswertungen und Reports in einem Konzept niederschreiben
- Auf die Attraktivität und Usability der Plattform achten
- Eigene Module können in kleiner Anzahl mit eingestellt werden

MVV Energie AG
Luisenring 49
68159 Mannheim

gerhard.voelkner@mvv.de

Ein Unternehmen in der Metropolregion Rhein-Neckar