bdew

Energie. Wasser. Leben.

CYBERSICHERHEIT IN DER ENERGIE- UND WASSERWIRTSCHAFT

FAKTOR MENSCH:

Die Unternehmenssicherheit mit geschulten Mitarbeitern stärken

Inhalt

Testimonials

Durch die Teilnahme an Schulungen zur Informationssicherheit bin ich für Risiken bei der täglichen Arbeit in der Leitstelle sensibilisiert und kenne aktuelle Bedrohungsszenarien z.B. im Bereich Social Engineering.

Benjamin Woboril,
Teamleiter Netzleitstelle Strom,
Netz Leipzig GmbH

Unsere für Cybersicherheit sensibilisierten und geschulten Mitarbeiter sind die erste Firewall im Smart Metering. Durch sicherheitsbewusstes und umsichtiges Verhalten identifizieren und melden unsere Mitarbeiter umgehend erkannte Cyberbedrohungen, bevor eine „echte" Sicherheitslücke entsteht oder ausgenutzt werden kann.

Nils Kraft,
Teamleiter Messstellenbetreiberprozesse,
EnBW Energie Baden-Württemberg AG

Impressum

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Susanne Zels
+49 (0)30 300 199 1675
susanne.zels@bdew.de

Yassin Bendjebbour
+49 (0)30 300 199 1526
yassin.bendjebbour@bdew.de

bdew
Energie. Wasser. Leben.

CYBERSICHERHEIT

DER BESTE SCHUTZ SIND IHRE MITARBEITER

Im Zuge der Digitalisierung der Energiewirtschaft nimmt die wertschöpfungsübergreifende Vernetzung von Vertrieb und Handel über die Erzeugung bis hin zu Netz und Verbrauch rasant zu. Diese Entwicklung wird durch den stetig wachsenden Anteil Erneuerbarer Energien und die Dezentralisierung noch weiter verstärkt. Auch für die Wasserwirtschaft stellt sich die Frage einer zunehmenden Digitalisierung und Vernetzung.

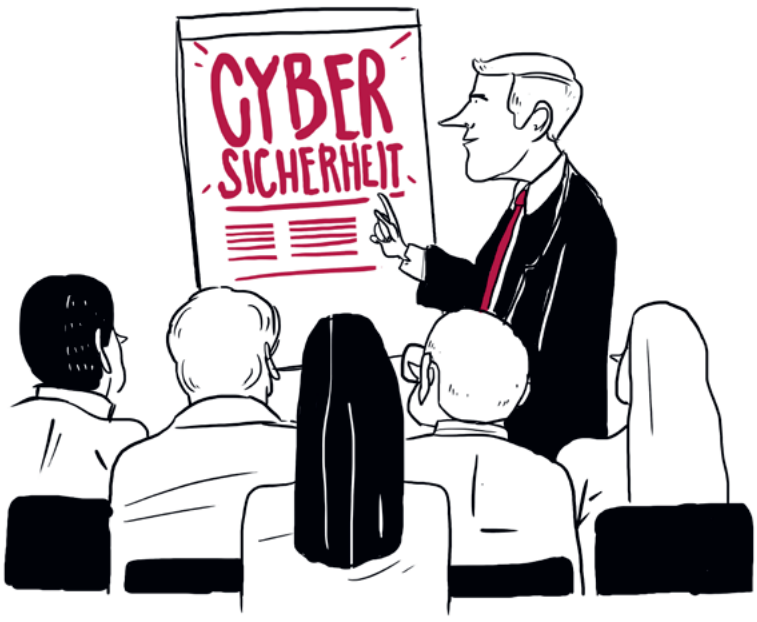
Diese Vernetzung ermöglicht die dringend benötigte effiziente, leistungsfähige und moderne Steuerung des Energiesystems und bringt darüber hinaus neue Chancen für datengetriebene und digitale Geschäftsmodelle. Mit der zunehmenden Digitalisierung werden jedoch auch die Risiken komplexer und mögliche Schadensauswirkungen deutlich höher.

Gehen beispielsweise bei einem Datenleck sensible Unternehmensdaten, Betriebs- und Geschäftsgeheimnisse oder Kundendaten verloren, können schnell hohe finanzielle Schäden entstehen. Auch Social-Engineering, CEO-Fraud oder Ransomware (z. B. Kryptotrojaner) können Unternehmen an empfindlichen Stellen treffen, wenn keine passenden Sicherheitsvorkehrungen getroffen wurden. Und nicht zuletzt trägt die Energie- und Wasserwirtschaft in unserer hochtechnologisierten Gesellschaft eine besondere Verantwortung für die störungsfreie Versorgung der Bevölkerung mit Strom, Gas, Fernwärme und Wasser.

Neben dem Begriff „Cybersicherheit“ häufig in diesem Zusammenhang genannte Begriffe sind unter anderem „IT-Sicherheit“, „Datensicherheit“ sowie in Fachkreisen „Informationssicherheit“. Während jeder dieser Begriffe einen unterschiedlichen Schwerpunkt setzt, haben alle von ihnen eines gemeinsam: sie sehen neben der rein technischen Absicherung auch personelle und organisatorische Maßnahmen vor, deren wichtigstes Ziel es ist, Mitarbeiter und Management des eigenen Unternehmens für Gefahren und verdächtige Situationen zu sensibilisieren.

Denn E-Mails oder manipulierte Webseiten stellen nach wie vor noch die mit Abstand häufigsten Infektionswege mit Schadsoftware dar[1] – ausgerechnet hier geraten technische Maßnahmen und Filter an ihre Grenzen. Regelmäßige Schulungen und interne Kommunikationskampagnen können stattdessen einen großen Beitrag für einen sicheren Umgang mit Unternehmensdaten leisten. Inhalte dieser Schulungen sollten der sichere Umgang mit Daten und Unternehmens-IT am Arbeitsplatz, auf Dienstreisen und im Home-Office sein. Die Sensibilisierung für den Umgang mit verdächtigen Situationen im E-Mailverkehr sowie bei der Nutzung von Internet sind ebenso von hoher Bedeutung für die IT-Sicherheit.

Der BDEW hat eine Checkliste der Sicherheitsvorkehrungen erstellt, die die Cybersicherheit in Ihrem Unternehmen stärken können. Prüfen Sie, welche dieser Maßnahmen bereits in Ihrem Unternehmen praktiziert werden und ob sie Bestandteil von Mitarbeiterschulungen sind.



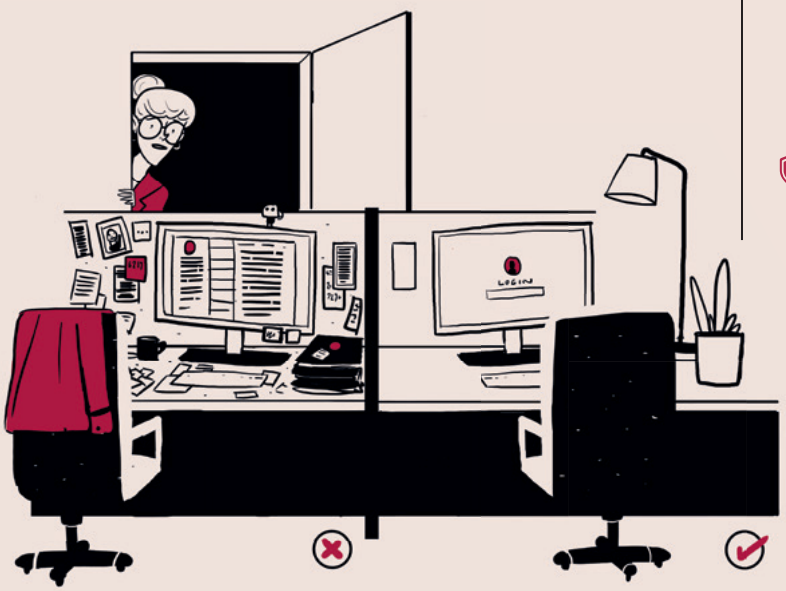
[1] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile

1

CYBERSICHERHEIT AM ARBEITSPLATZ

Der unbefugte Zugriff auf Unternehmensdaten und IT-Systeme kann physisch am Arbeitsplatz erfolgen. Deshalb ist es wichtig, dass Mitarbeiter für einen verantwortungsvollen Umgang mit Datenträgern, Ausdrucken und hinsichtlich des Zugangs Externer zum Arbeitsplatz geschult werden.

- Entsorgen Sie nicht mehr benötigte Dokumente und Speichermedien sicher und gemäß den unternehmenseigenen Regelungen.
- Räumen Sie sensible Dokumente immer vom Tisch und verwahren Sie sie sicher. Hinterlassen Sie den Arbeitsplatz aufgeräumt („Clear Desk“ Prinzip).
- Nutzen Sie für die Ablage von Dateien immer, wenn möglich die dafür bereitgestellten Server- und Netzwerklaufwerke. So ist sichergestellt, dass bei einem technischen Defekt oder bei Verlust ein Backup vorhanden ist.
- Sperren Sie bei Abwesenheit vom Arbeitsplatz den Zugriff auf Betriebssysteme (Windows-Taste + L).
- Sichern Sie Laptops und Tablets durch die Verwendung der Docking Stations oder eines Kensington-Schlosses.
- Tragen Sie Mitarbeiterausweise immer gut sichtbar. Sprechen Sie fremde oder unbekannte Personen an und bieten Sie ihre Hilfe an.
- Melden Sie externe Gäste an und lassen sie sie in Sicherheitsbereichen nicht unbeaufsichtigt.



- Hinterlassen Sie Besprechungsräume aufgeräumt, nehmen Sie Dokumente mit und sorgen Sie dafür, dass Flipcharts / Whiteboards gereinigt werden.
- Nutzen Sie für die Weitergabe von vertraulichen Informationen an den berechtigten Personenkreis einen verschlossenen Umschlag. Nutzen Sie für den Versand die Hauspost oder externe Botendienste.
- Informationssicherheit beim Faxen: Sprechen Sie den Versand schutzbedürftiger Informationen immer mit dem Empfänger ab, so dass dieser das Fax direkt nach der Übermittlung entgegen nehmen kann.
- Entnehmen Sie sensible Drucke sofort aus dem Drucker und verwenden Sie, wenn verfügbar, Drucker mit Authentifizierung (Secure Printing).
- Nutzen Sie für die Weitergabe von vertraulichen Informationen verschlüsselte Verbindungen oder verschlüsselte Datenträger.
- Stellen Sie sicher, dass vertrauliche Daten von Datenträgern unwiderbringlich gelöscht werden.
- Verwenden Sie sichere und schwer zu erratende Passwörter. Schreiben Sie diese nach Möglichkeit nicht auf und geben Sie Ihr Passwort niemals weiter. Vornamen und Geburtstage von Familien-angehörigen sind u.U. leicht zu erraten. Achten Sie darauf, auch Sonderzeichen und Groß- und Kleinschreibung zu verwenden.
- Schließen Sie Ihr Fenster nach Feierabend, verstauen Sie private Wertgegenstände sicher.

UMGANG MIT BEOBACHTUNGEN ODER SICHERHEITSVORFÄLLEN

Was tun, wenn doch mal etwas passiert oder Sie nicht sicher sind, was zu tun ist? Bereiten Sie Mitarbeiter auf den Umgang mit Sicherheitsvorfällen ihm Rahmen von Schulungen oder durch Informationskampagnen vor.

- Melden Sie verdächtige E-Mails, Anhänge oder Webseiten sowie ungewöhnliche System-meldungen umgehend an Ihren zuständigen Informationssicherheitsbeauftragten oder die IT-Abteilung.
- Wenn Sie unsicher sind, ob eine E-Mail, ein Anhang oder eine Webseite sicher sind, zögern Sie nicht, Ihren zuständigen Informationssicherheitsbeauf-tragten oder Ihre IT-Abteilung anzusprechen.
- Melden Sie Sicherheitsvorfälle wie z.B. Infektionen mit Malware, Verlust oder Diebstahl von Firmen-eigentum oder vertraulichen Informationen oder unberechtigte Zugriffe und Zutritte sowie versuchte Informationsabfluss via Telefon oder E-Mail umgehend an Ihren zuständigen Informationssicherheitsbeauftragen oder an die IT-Abteilung.
- Schließen Sie gefundene Hardware, wie z. B. USB-Sticks oder externe Festplatten, nicht ungeprüft an Ihren PC an. Melden Sie den Fund an Ihren zuständigen Informationssicherheits-beauftragten oder an die IT-Abteilungen.
- Sprechen Sie Kollegen in einem persönlichen Gespräch an, wenn Sie unachtsames oder unvorsichtiges Verhalten bei ihnen beobachten.

3

SOCIAL ENGINEERING

Social Engineering beschreibt eine Angriffsmethode, bei der sich Kriminelle durch die Manipulation von Mitarbeitern Zugang zu sensiblen Informationen eines Unternehmens oder einer Privatperson verschaffen. Das Risiko für diese Methode steigt zunehmend durch die verbreitete Nutzung von sozialen Netzwerken und Möglichkeiten, sich im Internet mit Unbekannten auszutauschen. Das Risiko vor Social Engineering-Angriffen kann durch ein gesundes Misstrauen bzw. durch sicherheitsbewusstes Verhalten im Alltag verringert werden.

- Wenn Sie bei Telefonaten unsicher sind, ob Ihr gegenüber auch die Person ist, für die er oder sie sich ausgibt, nutzen Sie Kontrollfragen.
- Bei telefonischer Aufforderung, Informationen über das Unternehmen oder über Kollegen herauszugeben, verweisen Sie den Anrufer darauf, eine schriftliche Anfrage zu stellen (mit Begründung, Aktenzeichen, etc.). Geben Sie niemals persönliche Daten Ihrer Kollegen an unbekannte Personen weiter.
- Informieren Sie sich über übliche Social Engineering Methoden: Gefährdungsszenarien beinhalten z.B. Phishing E-Mails sowie den sog. CEO-Fraud. Weitere Informationen finden Sie z.B. unter **www.bsi-fuer-buerger.de** .
- Seien Sie bei fremden Anrufern (auch Besuchern) achtsam.
- Reagieren Sie niemals auf Anfragen mit unrealistischen Versprechen und seien Sie misstrauisch bei Aufforderungen, Ihre persönlichen Daten herauszugeben.
- Geben Sie persönliche und sensible Firmendaten (Kontodaten, firmeninterne/-relevante Informationen wie längere Abwesenheit aufgrund von Urlaub) niemals an nicht-autorisierte Personen weiter.
- Überprüfen Sie die Privatsphäre-Einstellungen in sozialen Netzwerken darauf, welche Inhalte des Profils öffentlich einsehbar sind.
- Akzeptieren Sie keine Freundschafts-/Kontaktanfragen von unbekannten Personen bzw. prüfen Sie, ob widersprüchliche Aussagen im Profil verdächtig sind.
- Verwenden Sie private Zugangsdaten für Social Media-Profile nicht für andere Anwendungen im Unternehmen.

CYBERSICHERHEIT IM INTERNET UND BEI E-MAILS

Ein verbreitetes Einfallstor für Cybersicherheitsvorfälle ist Schadsoftware aus dem Internet und in E-Mails. Diese kann sich in Downloads und E-Mail-Anhängen verbergen und gut getarnt, beispielsweise als Bewerbungsunterlagen, und daher nur schwer erkennbar sein. Neben dem Einsatz von Virenscannern sollten Sie Ihre Mitarbeiter dafür sensibilisieren, welche aktuellen Risiken es zu beachten gilt.

- Nutzen Sie Ihre geschäftliche E-Mail-Adressen nicht für private Aktivitäten.
- Öffnen Sie keine E-Mail Anhänge von unbekannten oder verdächtigen Absendern. Seien Sie auch bei vermeintlich bekannten Absendern wachsam beim Öffnen von E-Mail-Anhängen.
- Klicken Sie in E-Mails von unbekannten Absendern auf keine Links – Rufen Sie die Webseite lieber selbst im Browser auf. Wenn Sie unsicher sind, rufen Sie den Absender an und lassen Sie sich die Authentizität bestätigen.
- Überprüfen Sie E-Mail-Absenderadressen und Links in E-Mails, da beispielsweise durch die Fälschung vertrauenswürdiger Adressen oder Hostnamen in Netzwerkprotokollen eine falsche Identität vorgetäuscht werden kann.
- Nutzen Sie Internet-Services wie Google-Übersetzer nicht für vertrauliche Daten – schon gar nicht per „Copy&Paste“.
- Verschlüsseln Sie vertrauliche Daten beim Versand via Email an Empfänger außerhalb der Organisation.

CYBERSICHERHEIT BEIM MOBILEN ARBEITEN

Durch die Schulung gesonderter Maßnahmen kann auch die Sicherheit der Unternehmens-IT auf Dienstreisen und im Home-Office verbessert werden.

- Lassen Sie mobile Endgeräte (Smartphones, Tablets, Laptops) nie unbeaufsichtigt. Sperren Sie die Geräte bei Nichtnutzung mit einem sicheren Verfahren.
- Vermeiden Sie die Nutzung öffentlich zugänglicher IT für dienstliche Kommunikation. Nutzen sie für ihre Devices im besten Fall eine Verschlüsselung oder sichere Containerlösungen für den E-Mail-Versand.
- Verwenden Sie eine Blickschutzfolie.
- Prüfen Sie unterwegs mit einem Schulterblick, ob jemand mitliest oder zuhört.
- Vermeiden Sie sensible Gespräche am Telefon oder mit Kollegen in der Öffentlichkeit.
- Verwenden Sie USB-Sticks und externe Speichermedien nicht sorglos als Backup-Medium. Verschlüsseln Sie ggf. vertrauliche Daten und beachten Sie diesbezügliche Regelungen Ihres Unternehmens.
- Melden Sie Diebstahl und Verlust mobiler Endgeräte unverzüglich.
- Verwenden Sie nur die vom Unternehmen vorgesehenen und freigegebenen Möglichkeiten zum Fernzugriff.
- Stellen Sie Firmenhardware (Laptop, Tablet, Speichermedien etc.) nie Unberechtigten zur Verfügung und lassen Sie sie nicht sichtbar im Auto liegen.
- Beachten Sie bei Auslandsdienstreisen auch länderspezifische Reisehinweise, z.B. des Auswärtigen Amtes.
- Sichern Sie Ihren privaten WiFi-Router zu Hause durch ein starkes Passwort und eine WPA2-Verschlüsselung.
- Vernichten Sie nicht mehr benötigte Papierdokumente wie Briefe und Arbeitsunterlagen sicher (schreddern und nicht im Hausmüll entsorgen).