Risikobasierte Awarenessbildung

Effektive Schulungen für den Mittelstand nach NIS2

Ich grüße Sie!

- Ursprünglich verantwortlich für den Betrieb komplexer IT-Infrastrukturen
- Awareness-Berater seit 2017
- Sensibilisierung von 5-Personen-Unternehmen bis hin zu den kritischsten Infrastrukturen des Kontinents
- Mitgründer der Marke SECUTAIN

Häufige Situation im Mittelstand

- „Die NIS2-Richitlinie ist am Horizont – aber wie soll ich mit ihrer Umsetzung anfangen? Eine ISO 27001-Reife überfordert uns.“
- „Das Budget für IT-Sicherheit ist sehr begrenzt. Für Sensibilisierung haben wir gar kein Budget.“
- „Notwendige Skills für eine Sensibilisierungsplanung, -durchführung und das dazu gehörige Reporting fehlen uns.“

Was fordert NIS2 in Bezug auf Awareness?

- Allen Mitarbeitenden müssen regelmäßige Schulungen zum Thema Informationssicherheit angeboten werden
- Führungsebenen müssen Schulungen zur Informationssicherheit wahrnehmen
- Die (Awareness)-Maßnahmen müssen den identifizierten Risiken in ihrer Eintrittswahrscheinlichkeit und/oder ihrem Schadenausmaß entgegenwirken. #Wirksamkeit

Was lässt die NIS2-Richtlinie offen?

- **Intervalle und Häufigkeit**: monatlich, jährlich, etc.
- **Tiefe & Umfang**: Die Richtlinie verlangt, dass Schulungen „ausreichende Kenntnisse und Fähigkeiten“ vermitteln, aber lässt viele Details offen (welche Themen, wie praxisnah, wie lang, etc.)
- **Methodik / Format**: Ob Präsenzseminar, Onlinekurs, Workshops, Gamification, Rollenspiele usw. – das bleibt Gestaltungsspielraum
- **Rollenbezogenheit**: Aufbereitung von Inhalten und Schwerpunkten für bestimmte Zielgruppen

Daraus folgt...

„Muss ich jetzt eine Sicherheitsschulung geben?“


Okay, Ingo. Die Sicherheitsschulung könnte etwas zu anspruchsvoll für Dich werden.
Ich weiß. Ich bin Ingo.
Ich heiße nicht Ingo.

Agenda

1 **Risikobasierte Schulungskonzepte**

Wie definieren Führungskräfte die Themen mit der höchsten Priorität für ihre Belegschaft?

2 **Effiziente Ressourcenplanung**

Strategien, um mit begrenzten Mitteln effektive und zielgerichtete Schulungsmaßnahmen umzusetzen

3 **Best Practices und Stolpersteine**

Dos und Don’ts für die Planung und Durchführung wirkungsvoller Sensibilisierungsmaßnahmen

Haben wir überhaupt Risiken?
Wer soll von uns schon etwas wollen?

Methode 1

Stellen Sie sich so auf, dass Sie möglichst viele der folgenden Fragen mit „Ja“ beantworten.

Die fünf Bausteine der NIS2-Richtlinie

- Cybersecurity Governance / ISMS
- Cybersecurity Prävention
- Vorfallsmanagement
- Business Continuity Management
- Zusammenarbeit mit den zuständigen Behörden

Was hat das mit meinem Mitarbeitenden zu tun?

Cybersecurity Prävention

- Wissen Ihre Mitarbeitenden um den Wert von geschützten Informationen für den Fortbestand und die Handlungsfähigkeit Ihrer Organisation?
- Kennen, verstehen und leben Ihre Mitarbeitenden die Richtlinien zur Informationssicherheit?
- Können sich Mitarbeitende auf die Unterstützung ihrer Führungskraft und des Top-Managements verlassen, wenn es um Sicherheit geht?
- Kennen Ihre Mitarbeitenden die informationellen Kronjuwelen, mit denen sie jeden Tag umgehen?

Cybersecurity Govern ISMS | Vorfallsmanagem | Business Continui Management | Zusammenarbeit mit den zuständigen Behörden

Was hat das mit meinem Mitarbeitenden zu tun?

Cybersecurity Governance / ISMS

- Sind Ihre Mitarbeitenden von den Sicherheitsmaßnahmen in Ihrer Organisation überzeugt?
- Wissen Ihre Mitarbeitenden, wie sie mit Schuldgefühlen umgehen?
- Wissen Ihre Mitarbeitenden, welche Informationen sie wem am Telefon oder per Mail geben können?

Cybersecurity Präve | Vorfallsmanagem | Business Continui Management | Zusammenarbeit mit den zuständigen Behörden

Was hat das mit meinem Mitarbeitenden zu tun?

Vorfallsmanagement

- Kennen Ihre Mitarbeitenden die Meldewege?
- Haben Ihre Mitarbeitenden die Möglichkeit, sich über aktuelle Bedrohungen und Risiken informiert zu halten?
- Können Ihre Mitarbeitenden unkompliziert verdächtige E-Mails melden?

Cybersecurity Governa
ISMS

Cybersecurity Präve

Business Continui
Management

Zusammenarbeit mit den zuständigen Behörden

Methode 2

Orientieren Sie sich an den aktuellen Top-Cyber-Risiken

Aktuelle Top-Risiken

Aktuell

- Phishing-E-Mails – insbesondere vor dem Hintergrund KI-generierter Mails
  - KI-basierte Recherche
  - LLM-basierte Szenarienentwicklung
  - Individueller Versand

1 Mail 150 Mal versenden

150 Mails 1 Mal versenden

KI

Aktuelle Top-Risiken

Aktuell

- Betrugsversuche
  - In der Schweiz aktuell über 50% der gemeldeten Cyberangriffe
  - Angriffe, die zum Ziel haben, dass eine mitarbeitende Person Stammdaten verändert

Das C-Level

Schritt 1: Mail mit Infos zu bevorstehendem Merge eines Dienstleisters

Von **CEO** peter.bauer@firna-online.de

CC **CFO** **CTO** hans.kleuber@firna-online.de

An **Finance** **Finance** **Legal** **Procurement** **Procurement** firma-online.de

Hallo zusammen,

In unserem Großprojekt steht einer unserer wichtigsten Dienstleister kurz vor einem Merge mit einer anderen Organisation. Aus bilanztechnischen Gründen hat der Dienstleister angefragt, ob die Möglichkeit besteht, die nächste Rechnung auf ein separates Konto zu überweisen. Da wir seit vielen Jahren vertrauensvoll und kooperativ zusammenarbeiten und wir im Großprojekt auf die fortwährenden Leistungen des Dienstleisters auch während seiner Transition angewiesen sind, bitte ich euch, Wege zu eruieren, dies umzusetzen.

Die Organisation wird tätig

Von	Procurement				
CC	CFO	CTO			
An	CEO	Finance	Finance	Legal	Procurement

Die Angreifer lesen die ganze Zeit mit

Von	Legal				
CC	CFO	CTO			
An	Procurement	CEO	Finance	Finance	Procurement

Externe Dienstleister werden hinzugezogen

Von Finance

CC CFO CTO

An Legal Procurement CEO Finance Procurement

Consulting Anwalt

Auch die externen erkennen den Betrug nicht

Von **Consulting**

CC **CFO** **CTO**

An **Finance** **Legal** **Procurement** **CEO** **Finance**
Procurement **Anwalt**

Die Täter werden nur aktiv, wenn etwas in die falsche Richtung geht oder langsamer wird.

Von **CTO**

CC **CFO**

An **Consulting** | **Finance** | **Legal** | **Procurement** | **CEO**

Finance | **Procurement** | **Anwalt**

Mit jeder neuen Nachricht, erhält die Konversation mehr Reputation.

Von	Anwalt				
CC	CFO				
An	CTO	Consulting	Finance	Legal	Procurement
	CEO	Finance	Procurement		

Die Security-Systeme geben Alarm. Die Domain ist mittlerweile «suspicious».

Von	Anwalt					
CC	CFO					
An	CTO	Consulting	Finance	Legal	Procurement	
	CEO	Finance	Procurement			

Kurz vor der Ausführung der Stammdatenänderung schlagen die IT-Sicherheitssysteme Alarm. Die Fake-Domain wird mittlerweile als gefährlich («suspicious») eingestuft. Wahrscheinlicher Grund: Mit der Domain wurden gleichzeitig weitere Angriffe durchgeführt, so dass die Domain gemeldet wurde.

Aktuelle Top-Risiken

Perspektivisch

- Deepfakes
  - Technik wird erschwinglicher und bedarf immer weniger Fachwissen
  - Toolchains werden aufgebaut, die durch Angreifende genutzt werden können

Aktuelle Top-Risiken

Aktuell

- Social Engineering
  - Zwischenmenschliche Manipulation
  - Per Mail, Telefon, im direkten Kontakt etc.
  - Umgang mit emotional aufgeladenen Situationen

Methode 3

Investieren Sie zwei Stunden in die Übersicht Ihrer Risiken

2 Stunden Mini-Schutzbedarfsanalyse

Setzen Sie sich mit 2-3 Wissensträgern zusammen und besprechen folgende Fragen:

- Mit welchen wichtigen Informationen gehen Sie um?
- Wo werden diese Daten aufbewahrt?
- Was bedeutet ein Verlust, Manipulation oder Diebstahl?
- Wie könnte dieses Risiko eintreten?

2 Stunden Mini-Schutzbedarfsanalyse

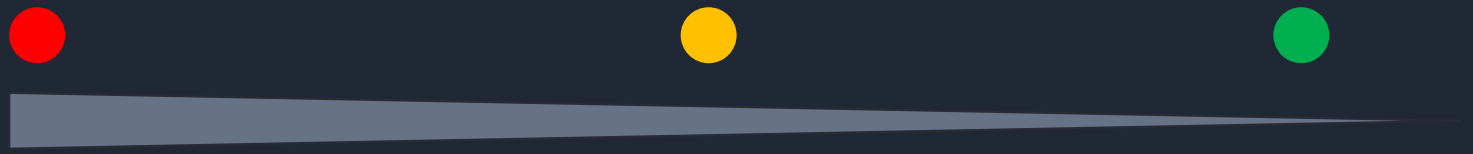
Kategorie	Beispiel	Verlust/ Manipulation oder Diebstahl bedeutet	Wahrscheinliche Risiken
Kundendaten	Daten im CRM, Excel-Listen	• Reputationsverlust • Meldepflichtiger Datenschutzvorfall	• Phishing ggf. mit Einschleusen von Malware (Verschlüsselung)
Geschäftsgeheimnisse	Verträge, Angebote, Projektdateien	• Wettbewerbsnachteil • Rechtliche Ansprüche	• Unkontrollierte Nutzung von Cloud-Anwendungen • Vishing-Anrufe
Kommunikation	E-Mails, Unternehmenschats	• Informationen für tiefergehende Angriffe • Reputationsverlust	• Phishing • Shoulder Surfing im öffentlichen Raum

Risiken priorisieren nach Schadensausmaß und Eintrittswahrscheinlichkeit

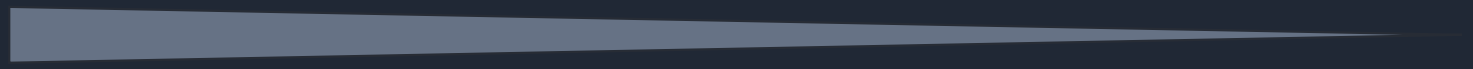
- Rot (hoch) = unmittelbare Auswirkung auf Geschäftsbetrieb oder Reputation, existenzgefährdend
- Gelb (mittel) = spürbar, aber kontrollierbar
- Grün (gering) = nervig, aber nicht geschäftsentscheidend

2 Stunden Mini-Schutzbedarfsanalyse

Risikobewertung



Menschliches Verhalten



Gewichtete Sensibilisierungsschwerpunkte:

1. Phishing-Abwehr
2. Sensibilisierung gegen Betrugsversuche
3. Social Engineering

Agenda

1 **Risikobasierte Schulungskonzepte**

Wie definieren Führungskräfte die Themen mit der höchsten Priorität für ihre Belegschaft?

2 **Effiziente Ressourcenplanung**

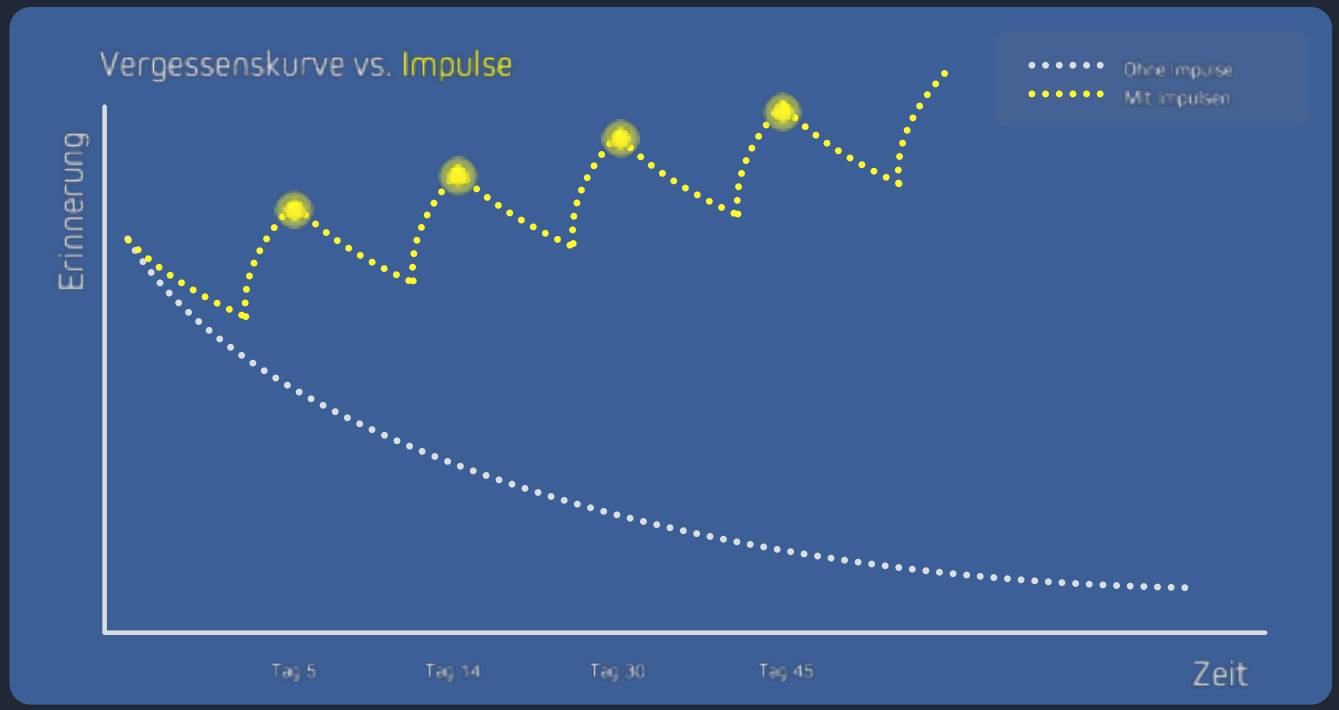
Strategien, um mit begrenzten Mitteln effektive und zielgerichtete Schulungsmaßnahmen umzusetzen

3 **Best Practices und Stolpersteine**

Do’s und Don’ts für die Planung und Durchführung wirkungsvoller Sensibilisierungsmaßnahmen

Ich habe neulich ein Live-Hacking gesehen! Das müssen wir bei uns auch mal machen!

Der Vergessenskurve entgegenwirken



Dauerhafte Sichtbarkeit

erhöht die Chance, dass das Thema als strategisch relevant wahrgenommen wird

Kein Sprint sondern ein Triathlon

Eine Schulung ist kein Patch, den man in eine Organisation einspielt.

Nachhaltige Handlungsanpassung

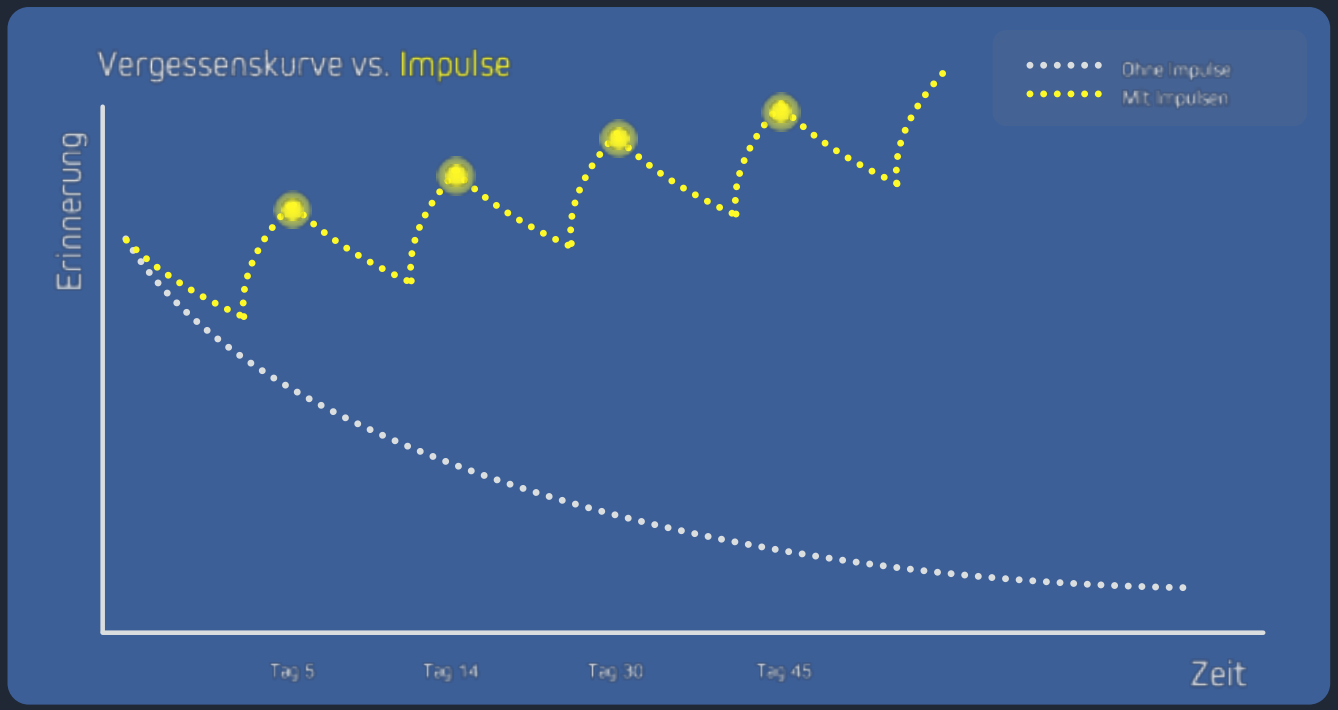
Die kognitive Ebene
Das „Wissen“ um die Sache, also im Bereich Informationssicherheit die Kenntnis über potenzielle Gefahren, die Relevanz der Informationssicherheit und entsprechende Richtlinien im Unternehmen.

Die emotionale Ebene
Sicherheit als positiv assoziiertes Gefühl etablieren anstatt als lästige Vorschriften, die den eigenen Handlungsraum einschränken.

Was können diese Impulse sein?

Vor dem Hintergrund

- Budgetknappheit
- Skills
- Personelle Ausstattung



Regelkommunikation

- Machen Sie Informationssicherheit zum Bestandteil der bestehenden Regelkommunikation
- Nutzen Sie Medien, die bei Ihnen etabliert sind
  - Je näher ein Thema an der Organisation ausgerichtet ist, desto eher sind Mitarbeitende bereit, sich mit dem Thema auseinanderzusetzen
  - Ggf. anonymisierte Aufbereitung
  - Aufbereitung von Vorfällen in Ihrer Organisation
  - Wenn das nicht möglich ist Beispiele aus der Branche oder der Region
  - Darstellung von sicherheitswahrendem Verhalten

E-Learnings

- Günstig am Markt einzukaufen
- Nach wie vor hohe Affinität für videobasiertes Lernen
- Sie können den Schwerpunkt bestimmen
- Verschiedene Anbieter bieten die Möglichkeit der inhaltlichen und optischen Anpassung an
- Machen Sie sich zunächst von der Art der Aufbereitung von Themen vertraut – das ist entscheidend für den Erfolg (Stichwort: Sympathie & Wissen)

- Vorteil: Nachweis der Teilnahme ist zumeist sehr einfach (wichtig für die Dokumentation für NIS2)

Webinare

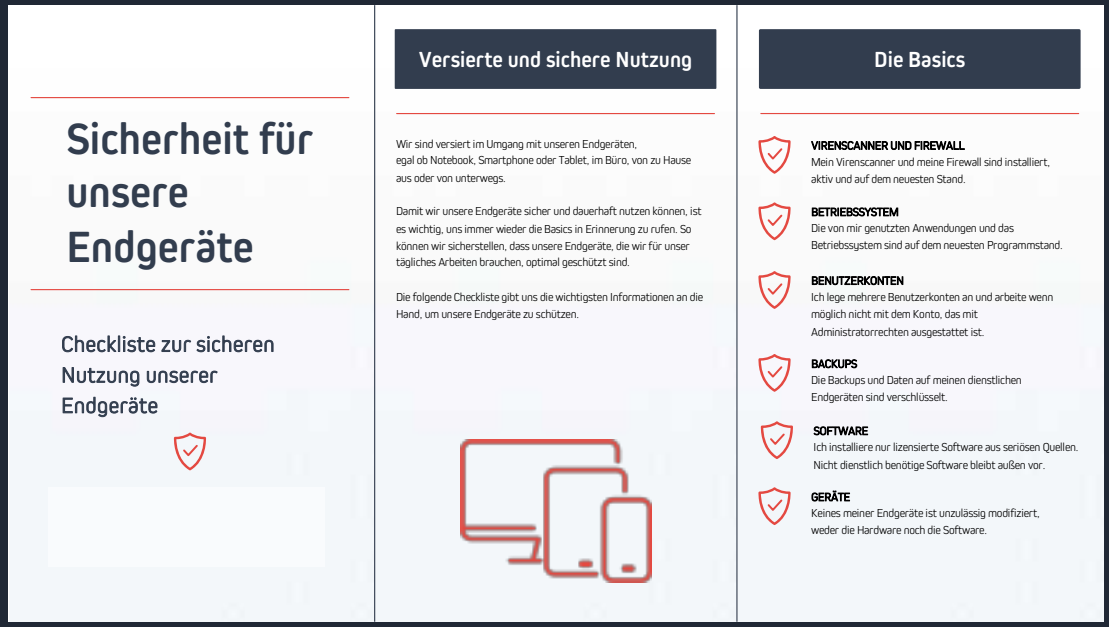
- Hohe Akzeptanz bei der Berücksichtigung der speziellen Eigenschaften des Mediums
  - Kurzweiligkeit
  - Immer wieder aktive Parts
  - Berücksichtigung der Ablenkung
  - Geringe Dauer
- Bestenfalls interne vortragende Person – zeigen Sie Gesicht!
- Viele Anbieter am Markt und recht günstig zu beschaffen
- Nachweis der Teilnahme möglich
- Mehrere Termine oder Aufzeichnungen anbieten

Phishing-Simulation

- Sehr effektives Mittel gegen das Cyberrisiko Nummer 1, wenn es überlegt und gut begleitet durchgeführt wird
- Open Source-basierte Plattform (GoPhish) oder bereits sehr günstige Einstiegsmodelle bei diversen Anbietern
- Erfolgskriterien:
  - Dauer,
  - Ankündigung,
  - Transparenz,
  - Nutzen des Moments der höchsten Lernbereitschaft etc.
- https://secutain.com/blog/10-tipps-damit-ihre-phishing-simulation-zum-erfolg-wird-teil-1/

Broschüren

- Übersichtliche Darstellung eines Schwerpunktes
- Leicht konsumierbar
- Als Download oder ausgedruckt
- Als Begleitung zu einem Webinar
- Leute lieben Checklisten



Sicherheit für unsere Endgeräte

Checkliste zur sicheren Nutzung unserer Endgeräte

Versierte und sichere Nutzung

Wir sind versiert im Umgang mit unseren Endgeräten, egal ob Notebook, Smartphone oder Tablet, im Büro, von zu Hause aus oder von unterwegs.

Damit wir unsere Endgeräte sicher und dauerhaft nutzen können, ist es wichtig, uns immer wieder die Basics in Erinnerung zu rufen. So können wir sicherstellen, dass unsere Endgeräte, die wir für unser tägliches Arbeiten brauchen, optimal geschützt sind.

Die folgende Checkliste gibt uns die wichtigsten Informationen an die Hand, um unsere Endgeräte zu schützen.

Die Basics

VIRENSCANNER UND FIREWALL
Mein Virenscanner und meine Firewall sind installiert, aktiv und auf dem neuesten Stand.

BETRIEBSSYSTEM
Die von mir genutzten Anwendungen und das Betriebssystem sind auf dem neuesten Programmstand.

BENUTZERKONTEN
Ich lege mehrere Benutzerkonten an und arbeite wenn möglich nicht mit dem Konto, das mit Administratorrechten ausgestattet ist.

BACKUPS
Die Backups und Daten auf meinen dienstlichen Endgeräten sind verschlüsselt.

SOFTWARE
Ich installiere nur lizensierte Software aus seriösen Quellen. Nicht dienstlich benötige Software bleibt außen vor.

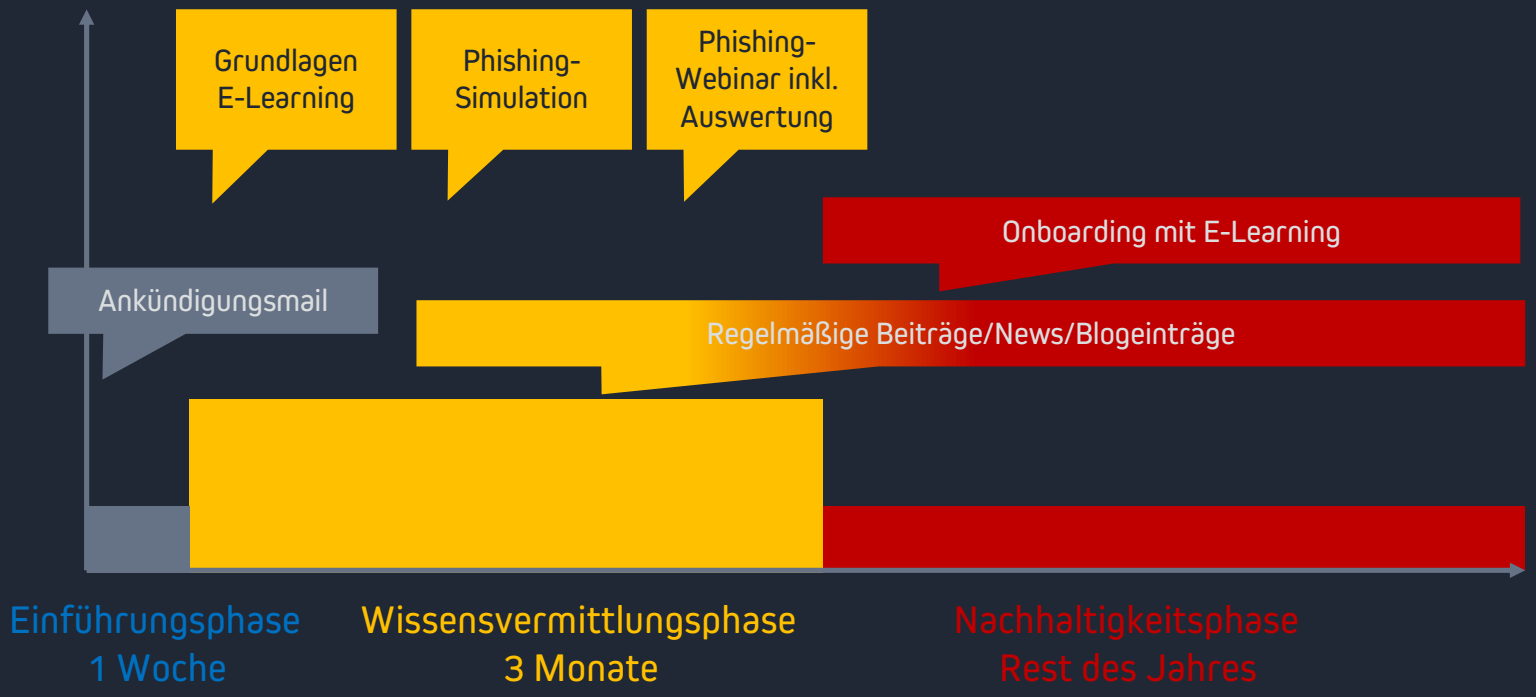
GERÄTE
Keines meiner Endgeräte ist unzulässig modifiziert, weder die Hardware noch die Software.

Aufbau einer Anlaufstelle

Egal, was Sie tun, sammeln Sie die Ergebnisse an einer zentralen Stelle (Teams-Kanal, Wiki-Seite, Intranet-Seite, Aushang etc.)

- Archiv veröffentlichter Texte/News
- Aufgezeichnete Webinare
- Statistiken zur Phishing-Simulation
- Folien, Broschüren, Richtlinien
- Meldeweg/Kontaktmöglichkeit
- Guter Leistungsnachweis für NIS2

Mögliche Kampagne für ein KMU



Agenda

1 **Risikobasierte Schulungskonzepte**

Wie definieren Führungskräfte die Themen mit der höchsten Priorität für ihre Belegschaft?

2 **Effiziente Ressourcenplanung**

Strategien, um mit begrenzten Mitteln effektive und zielgerichtete Schulungsmaßnahmen umzusetzen

3 **Best Practices und Stolpersteine**

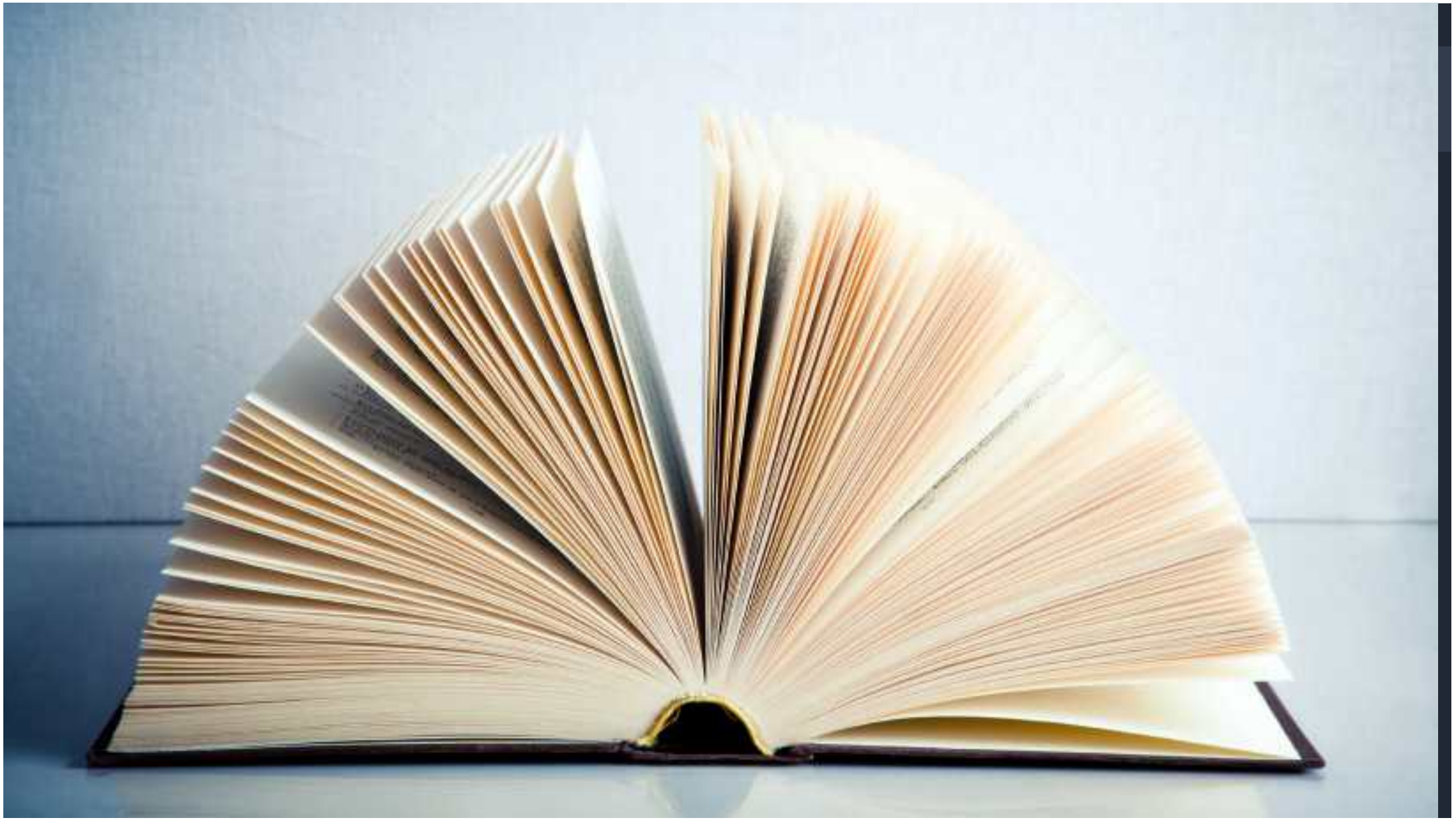
Do’s und Don’ts für die Planung und Durchführung wirkungsvoller Sensibilisierungsmaßnahmen

Thema Schwerpunkte

Passwort-Management	Informations-klassifizierung	Zutrittszonen	Verhalten in Sozialen Medien	Sichere Nutzung von KI
BYOD („Bring Your Own Device“)	Entsorgung und Vernichtung	Informations-übertragung	Lieferanten-Steuerung	Incidents bei Partnern
Verhalten im (halb-) öffentlichen Raum	Clear Desk (aufgeräumter Arbeitsplatz)	Besucher-Management	Mobiles Arbeiten	Betrugs-Angriffe
Homeoffice	Ransomware	Social Engineering	Datenschutz	KI-basierte Angriffe
Phishing	Deepfakes	Vishing	Reisesicherheit	Innentäter

Weniger ist mehr

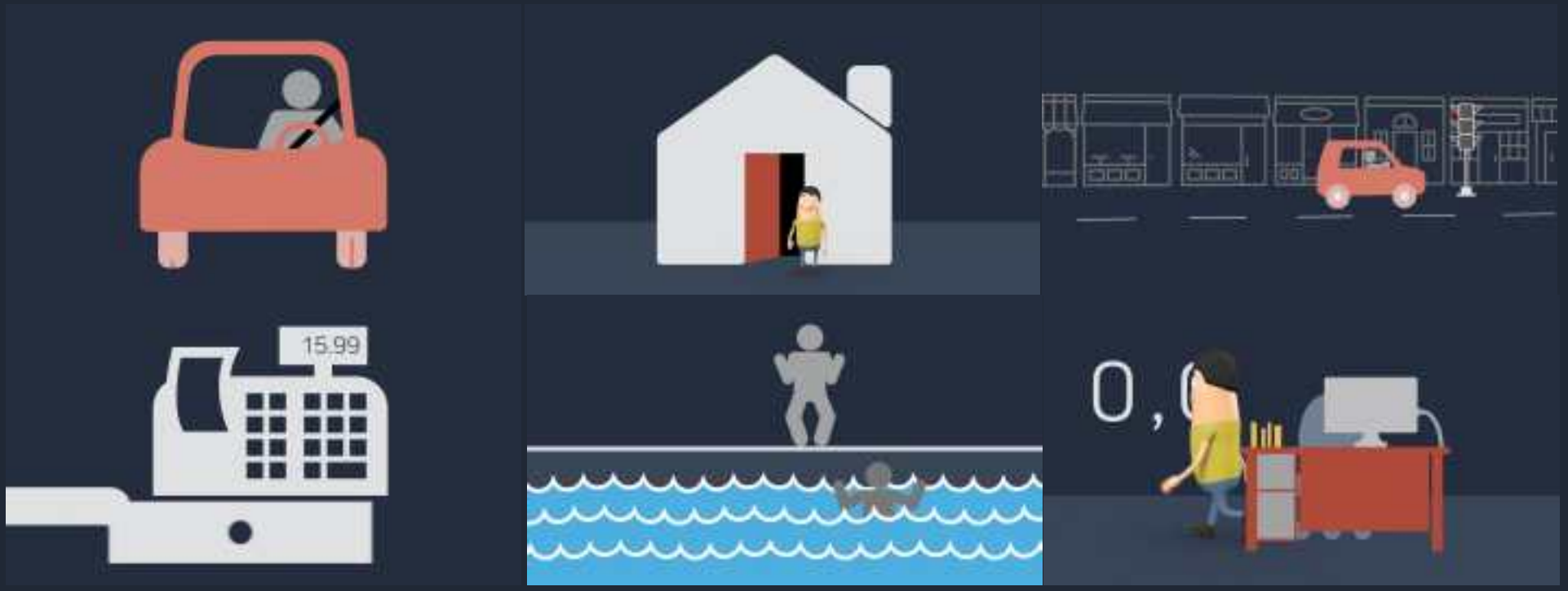
- Setzen Sie nicht zu viele Schwerpunkte
- 1-2 Schwerpunkte pro Jahr ist legitim
- 3-4 Schwerpunkte pro ist machbar
- Über 5 Schwerpunkte ist nicht zu empfehlen



Nutzen Sie die Macht des Storytellings

- Geschichten über mutige Pförtner, sich im E-Mail-Verkehr zurücklehnende Angreifer, Stadionbesuche und erdachte Freundinnen des Geschäftsführers erzeugen Aufmerksamkeit, bleiben über lange Zeit haften und holen das Thema Informationssicherheit aus der Technikecke heraus
- Wie lieben Dramen, Anekdoten und Heldengeschichten, die auf Fakten basieren.

Anschlussfähigkeit



Verständlichkeit geht vor Vollständigkeit

Es geht um Prinzipien – nicht um Edge-Cases.
Beispiel:

- Automatische Sicherheitsupdates
- Virtual Private Network
- https
- Mehrfaktorauthentifizierung etc.

sind alles technische Maßnahmen, die das Sicherheitsniveau erheblich steigern und deswegen zu empfehlen sind – und dennoch keine 100%ige Sicherheit versprechen. Die Darstellung der Edge-Cases, in denen diese Maßnahmen umgangen werden können, schädlich sein können oder ausgehebelt werden, sollte nicht im Zentrum der Kommunikation stehen.

Fachsprache

Die Informationssicherheit ist ein Bereich, der mit Fachsprache durchzogen ist.

- Gleiche Syntax für Experten (Gruppensprache)
- Effizienz
- Absonderung von den „Unwissenden“ (Kodierung)
- Darstellung des Fachniveaus
- Legitimierung eines Expertenstatus‘

Fachsprache

Vermeiden Sie, wo es geht, Fachbegriffe

Wenn es nicht anders geht, erklären Sie die Fachbegriffe oder bieten ein Glossar an.

Wenn wir verstanden werden wollen, müssen wir die kommunikative Erwartungshaltung unserer Zielgruppe treffen – und diese ist im seltensten Fall Fachsprache.

Besten Dank!


SECUTAIN
David Scribane
Leiter SECUTAIN
etomer GmbH
Winkler Straße 27
14193 Berlin
david.scribane@secutain.com
+49 170 2246938
secutain.com