Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Information Security Management
The Human Factor – Security Awareness

HSLU – Informatik

Marco Orefice (M.Sc.)

Tel. +41 79 357 42 86

Marco.orefice@axians.com

FH Zentralschweiz

EFQM
Recognised for excellence
5 star - 2015

Über mich

Marco Orefice

- BSc Information Science
- MSc Business Information Systems
- Consultant für IT/OT Cyber Security bei Axians

MSSP der die individuellen Bedürfnisse seiner Kunden kennt und einen ganzheitlichen Cyber Security Ansatz bietet.

Security Operation Center in Basel

Ziele

Die Studierenden

- erkennen die Wichtigkeit des “Human Factors” und messen Security Awareness eine hohe Bedeutung bei.
- kennen mögliche Vorgehensweisen für die Initiierung, Durchführung und Erfolgsprüfung einer Security Awareness-Kampagne und können diese anwenden.
- kennen die relevanten Erfolgsfaktoren von Security Awareness Training.

Informationssicherheit: Womit?

"Goldenes Dreieck"

- **Technik**: kaufen, konfigurieren
- **Prozesse**: definieren, kontrollieren
- **Mitarbeiter**: sensibilisieren, ausbilden

NIST Cybersecurity Framework

Agenda

1. **The Human Factor – was ist das?**
2. Warum Security Awareness Training?
3. Awareness Training planen und umsetzen
4. Demo: Security Awareness Training Tool / Shodan

The Human Factor

- **Human Factors in Cyber Security**: Wenn menschliche Fehler/menschliches Fehlverhalten zur Verletzung der Informationssicherheit führt.
- Der Mensch ist einer der grössten Risikofaktoren und damit gleichzeitig auch einer der grössten Schutzfaktoren.
- Die Mitarbeiter spielen eine entscheidende Rolle in der Informationssicherheit und beim Schutz der "Assets", auch technisch (der Mensch steuert und kontrolliert).
- Es kann zu vorsätzlichen, bewussten oder unbewussten Fehlhandlungen kommen.
- Security Awareness Training ist ein Hauptinstrument, um die Informationssicherheit zu verbessern.

…gleich zu Beginn ein Beispiel

Täter

- Frustrierte Mitarbeitende
- Geheimdienste, staatliche Akteure
- Industriespionage
- Hacker/Cracker
- Whistleblower
- Softwareentwickler (Back Doors)
- Fremdpersonal (externe MAs)
- Administratoren

Neue Zürcher Zeitung

KOMMENTAR

Staatsgeheimnisse in der Hand von leichtsinnigen Jugendlichen: Diese Grobfahrlässigkeit der Weltmacht USA muss Konsequenzen haben

Die Affäre um die Enthüllung von geheimen Pentagon-Papieren verblüfft nicht nur wegen des Hochrisiko-Verhaltens des mutmasslichen Täters. Sie entlarvt auch die mangelnde Vorsicht der politischen Verantwortlichen in Washington.

Andreas Rüesch
113 Kommentare →
14.04.2023, 11.41 Uhr

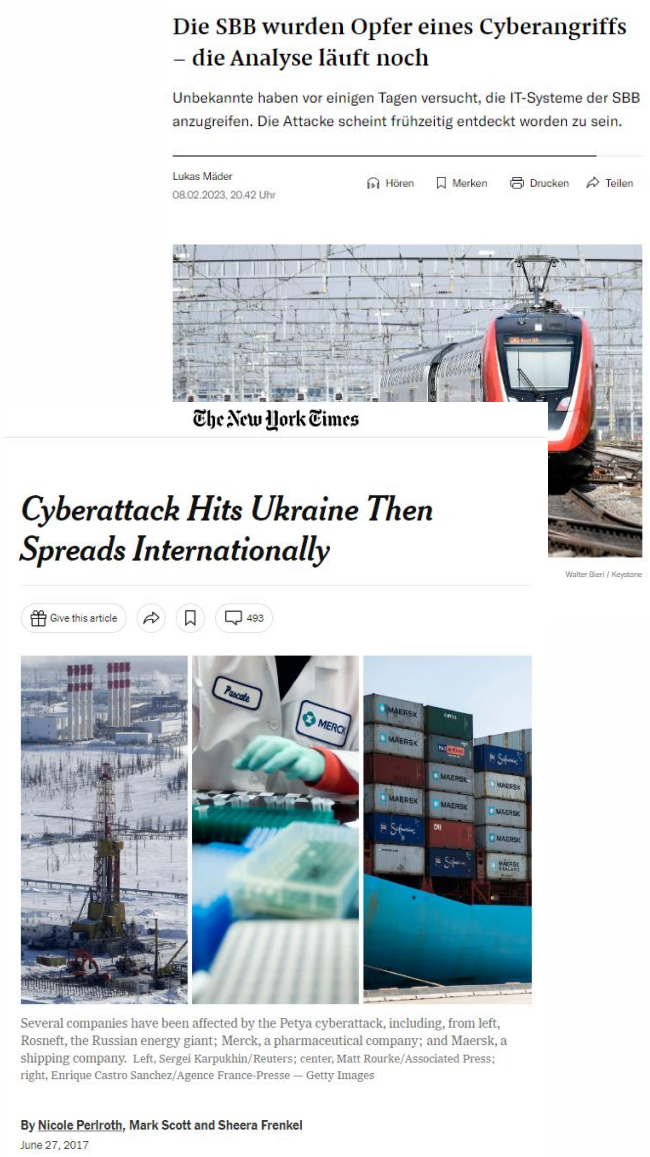
Hören Merken Drucken Teilen

Das Pentagon, das grösste Bürogebäude der Welt, präsentiert sich dem Auge wie eine Festung. Doch seine mit Aussenstationen rund um den Globus verbundenen Datenbanken sind nicht genug geschützt.

Joshua Roberts / Reuters

Vorsätzliche Manipulation

- Angriffe über das Internet
- Unerlaubter Zugriff auf Systeme
- Abhören und Modifizieren von Daten
- Angriff auf die Verfügbarkeit von Systemen
- Missbrauch von Systemen, Distributed Denial of Service (DDOS)
- Viren, Würmer und Trojanische Pferde
- Drive by Infection



Die SBB wurden Opfer eines Cyberangriffs – die Analyse läuft noch

Unbekannte haben vor einigen Tagen versucht, die IT-Systeme der SBB anzugreifen. Die Attacke scheint frühzeitig entdeckt worden zu sein.

Lukas Mäder
08.02.2023, 20.42 Uhr

Hören Merken Drucken Teilen

Walter Bieri / Keystone

The New York Times

Cyberattack Hits Ukraine Then Spreads Internationally

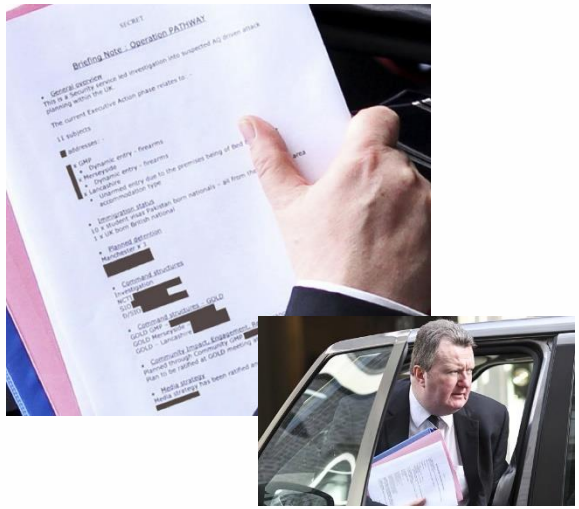
Give this article 493

Several companies have been affected by the Petya cyberattack, including, from left, Rosneft, the Russian energy giant; Merck, a pharmaceutical company; and Maersk, a shipping company. Left, Sergei Karpukhin/Reuters; center, Matt Rourke/Associated Press; right, Enrique Castro Sanchez/Agence France-Presse — Getty Images

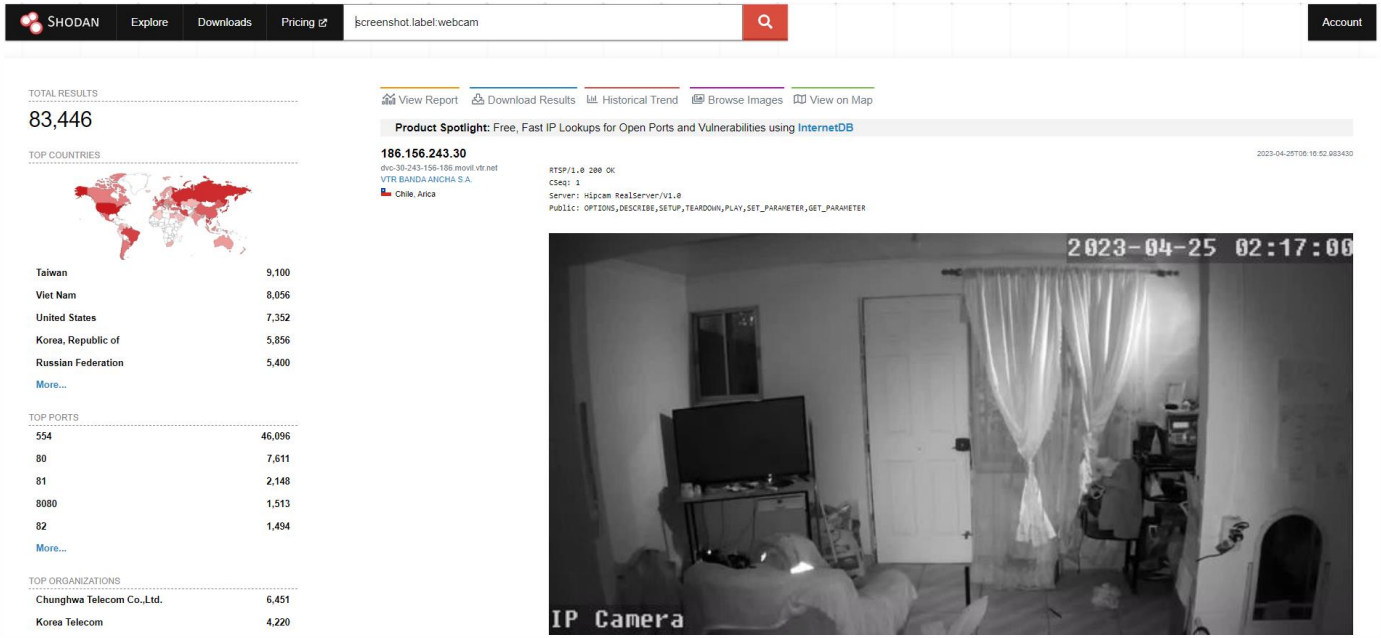
By Nicole Perlroth, Mark Scott and Sheera Frenkel
June 27, 2017

Menschliches Fehlverhalten

- Fahrlässigkeit
- Gleichgültigkeit
- Unwissenheit
- Leichtgläubigkeit



Bob Quick, ex Scotland Yard



Shodan.io
Beispiel Suchanfragen:
screenshot.label:webcam
screenshot.label:ics

Shodan is a search engine for Internet-connected devices.

- Google crawls the www (scans ports 80 & 443)
- Shodan crawls the internet (scans all ports)

Was gefährdet die Informationen? Welche Gefährdungen/Bedrohungen gibt es?

- Nicht vorsätzliche (zufällige) Gefährdungen/Bedrohungen
  - Naturgewalten (Blitz, Hagel, Unwetter, Erdrutsche, Hochwasser etc.)
  - Ausfall von Strom oder Telekommunikation
  - Technische Pannen, z.B. Fehler von Hard- und/oder Software
  - Bedienerfehler / Fahrlässigkeit der Mitarbeitenden

- Vorsätzliche Gefährdungen/Bedrohungen
  - Bösartiger Code (Viren, Würmer, Trojaner etc.)
  - Informationsdiebstahl
  - Angriffe (von Skript-Kiddies bis Hacker)
  - Wirtschaftsspionage („was die Konkurrenz wissen möchte ”)
  - Missbrauch der IT-Infrastruktur

Daten, Information und Wissen

„Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.“

Informationssicherheitshandbuch für die Praxis

„Information ist Wissen in Aktion.“

Rainer Kuhlen, 2004

Der Wert von Information

„Knowledge is Power. “
(Francis Bacon, 1561-1621)

„Information is the oil of the 21st century. “

Information ist wertvoll, da sie uns hilft unsere Ziele zu erreichen, oder – im Falle von Missbrauch – Schaden zufügen kann.

Agenda

1. The Human Factor – was ist das?
2. **Warum Security Awareness Training?**
3. Awareness Training planen und umsetzen
4. Demo: Security Awareness Training Tool / Shodan

Begriff «Awareness»

aware [ə'weə(r)] *adj.* **a)** *pred.* *(conscious)* **be ~ of sth.** sich *(Dat.)* einer Sache *(Gen.)* bewußt sein; **be ~ that ...:** sich *(Dat.)* [dessen] bewußt sein, daß ...; **as far as I am ~:** soweit ich weiß; **not that I am ~ of** nicht, daß ich wüßte; **b)** *(well-informed)* informiert

awareness [ə'weənɪs] *n., no pl.* *(consciousness)* Bewußtsein, *das*

awash [ə'wɒʃ] *pred. adj.* auf glei-

Warum Security Awareness Training?

- Zum Schutz der Informationen erlässt man eine Informationssicherheitsrichtlinie und stimmt diese mit den Anforderungen des Unternehmens, relevanten Gesetzen und Regulierungen ab.
- Aber … Auch die besten Sicherheitsrichtlinien sind nutzlos, wenn sie nicht gelebt werden.
- Das «what, who and why» muss and die Belegschaft kommuniziert werden, damit die Ziele und Anforderungen an die Informationssicherheit innerhalb einer Organisation erreicht werden können.

Frage: Was sind die grundsätzlichen Schutzziele?

→ CIA

Was wollen wir erreichen?

Was ist das Ziel von Security Awareness Trainings?

- Dass die Mitarbeiter die Wichtigkeit von Informationssicherheit für das Unternehmen sowie ihren individuellen Beitrag dazu verstehen.
- Dass die Verantwortlichkeiten und das erwartete Verhalten klar ist.
- Dass klar ist, was die Folgen der Nichteinhaltung sind.

Ziel ist es, das Verhalten und die Einstellung der Mitarbeiter zur Informationssicherheit zu ändern.

Charakter, Werte und Verhalten

- "Charakter":
  - Persönliche Kompetenzen, die die Voraussetzung für ein moralisches Verhalten bilden
  - Temperament bzw. dessen auffällige Verhaltensgewohnheiten
  - Wird teilweise durch die Gene vererbt und teilweise frühkindlich antrainiert.

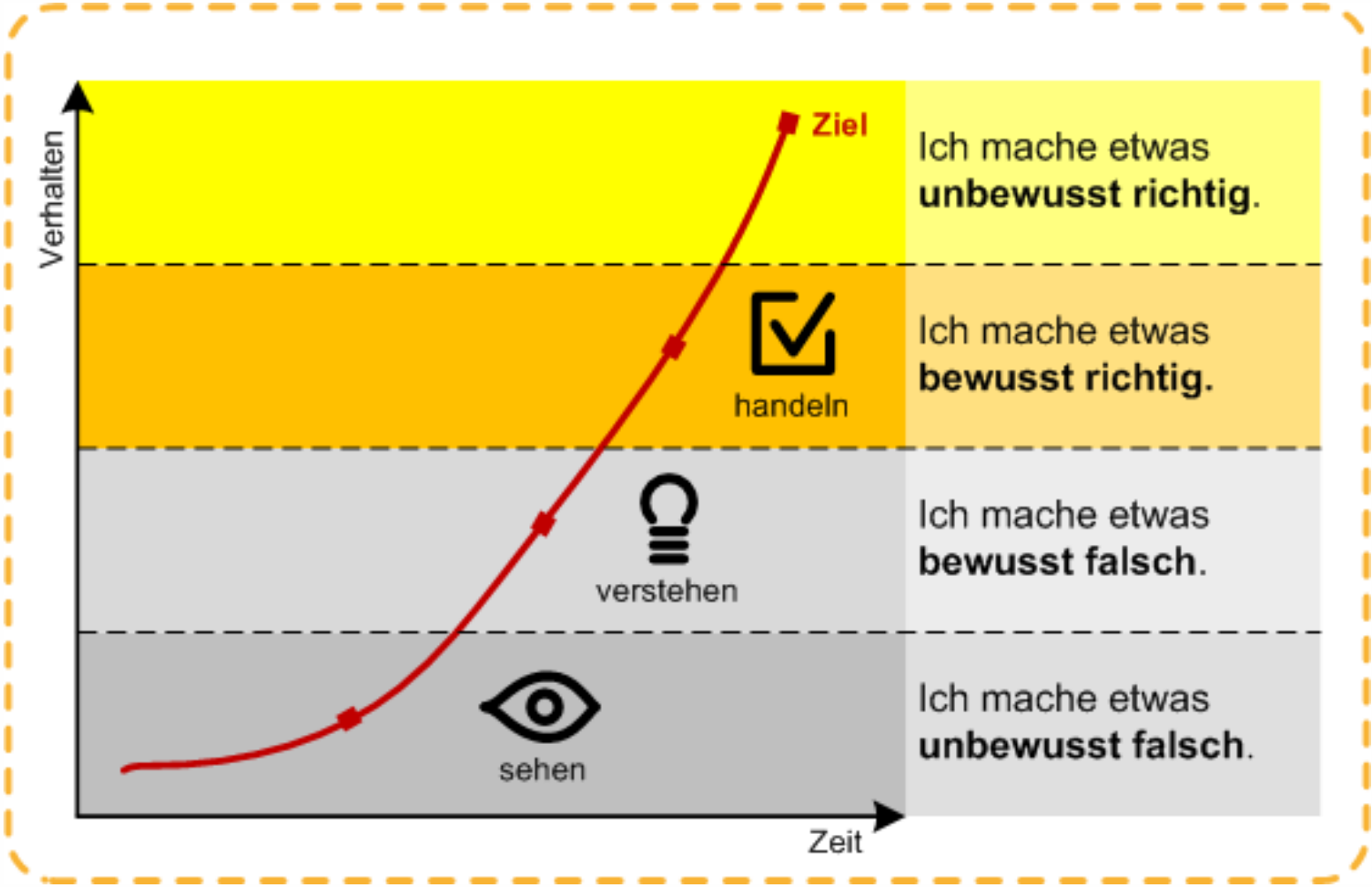
- *"Werte":* (Wertvorstellungen) sind allgemein erstrebenswerte, moralisch oder ethisch als gut befundene spezifische Wesensmerkmale einer Person innerhalb einer Wertegemeinschaft.

Charakter, Werte und Verhalten

- *„Verhalten":* Aus den präferierten Werten und Normen resultieren Denkmuster, Glaubenssätze, Handlungsmuster. In Folge entstehen Ergebnisse (Resultate, Erlebnisse, Erfolge), welche die gewünschten werthaltigen Eigenschaften besitzen oder vereinen sollen.

- Wie können wir Werte und schlussendlich das Verhalten positiv beeinflussen?
  - **Bewusstsein**: die Fähigkeit des Menschen zur Wahrnehmung des eigenen Ichs; sich des eigenen Handelns und dessen Auswirkung bewusst sein
  - **Berufsethik**: Wie übt man den Beruf professionell und "gut" aus?
  - **Berufsgeheimnis**: Schafft Vertrauensverhältnis, Schutz von Personen
  - **Empowerment**: Selbstbestimmung über die Umstände des eigenen Lebens (bzw. Berufslebens).
  - …

Prozess der Verhaltensänderung



Agenda

1. The Human Factor – was ist das?
2. Warum Security Awareness Training?
3. **Awareness Training planen und umsetzen**
4. Demo: Security Awareness Training Tool / Shodan

Herausforderungen

- Sicherheit umfasst viele verschiedene Aspekte eines Unternehmens und es kann deshalb schwierig sein, die richtigen Informationen an die richtigen Personen zu vermitteln.

- Datenschutz, Physische Sicherheit, Umgang mit Datenträgern und Dokumenten, Home Office, Passwortschutz, Umgang mit Mobilgeräten, Social Engineering, Incident Management …

- Spezielle Situation an einem Arbeitsort müssen berücksichtigt werden (z.B. Klinik, Bauunternehmung, Bank, Verwaltung, Transportunternehmen, Detailhandel und Vertrieb, Energieproduzent …)

Vorgehensweise

Mit einem formalisierten Prozesses für das Security Awareness Training kann sichergestellt werden, dass die relevanten Sicherheitsanforderungen an die richtigen Personen im Unternehmen vermittelt werden.

Z.B. NIST SP 800-12 Chapter 13 (Link).

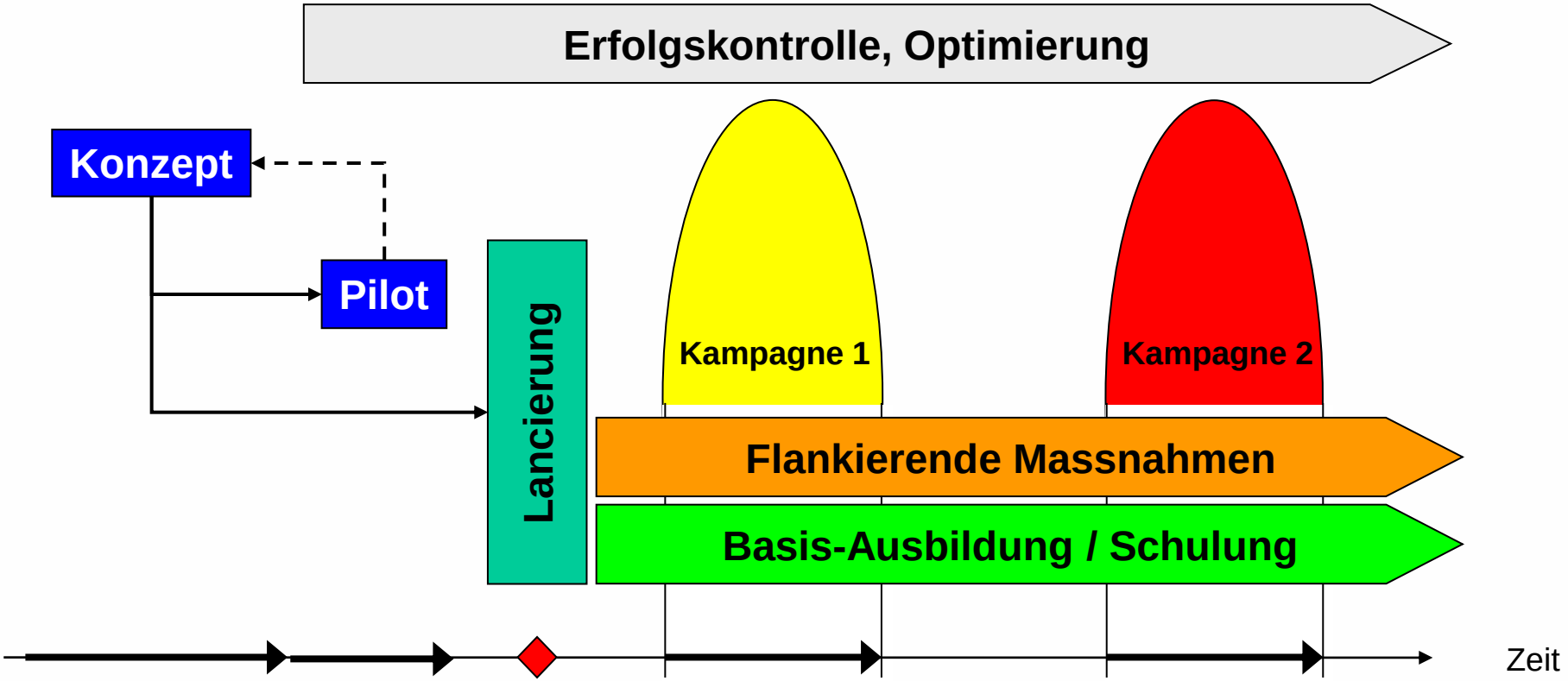
- Schritt 1: Umfang und Zielsetzung identifizieren
- Schritt 2: Trainer identifizieren
- Schritt 3: Zielgruppen identifizieren
- Schritt 4: Management und Mitarbeiter motivieren
- Schritt 5: Das Programm einführen und verwalten
- Schritt 6: Das Programm aktuell halten
- Schritt 7: Die Wirksamkeit des Programms evaluieren

Vorgehensweise

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Video - Newsletters - Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Harris, S. & Maymi, F. (2021). *CISSP All-in-One Exam Guide, Ninth Edition*.

Zeitlicher Ablauf eines Awareness-Programms



Erfolgsfaktoren – Stufengerecht schulen

- Ein Security Awareness Training richtet sich in der Regel mindesten an drei Arten von Zielgruppen: **Management, Benutzer/Anwender, technische Mitarbeiter**

- Die Schulung muss auf die einzelnen Zielgruppen zugeschnitten sein, um sicherzustellen, dass jede Gruppe ihre besonderen Verantwortlichkeiten, Verpflichtungen und Erwartungen versteht.

- Die höheren Schulungsebenen sind in der Regel allgemeiner gehalten und befassen sich mit breiteren Konzepten und Zielen. Je weiter die Schulung in Richtung spezifischer Arbeitsplätze und Aufgaben geht, desto situationsbezogener wird sie, da sie sich direkt auf bestimmte Positionen innerhalb des Unternehmens bezieht.

Erfolgsfaktoren – Erstellung der Inhalte

Die Inhalte für das Security Awareness Training sollten auf die Bedürfnisse der Organisation abgestimmt sein. Inhaltlich sollte es folgende Anforderungen erfüllen:

- umfassend, alle relevanten Inhalte abdecken
- die wichtigsten Botschaften auf verschiedene Arten transportieren (z.B. unterschiedliche Medien: Merkblatt, Video, Poster, Signatur, Game, Podcast …),
- unterhaltend, positiv, lustig, aktuell
- einfach verständlich (weniger ist mehr)

Hier kann man auf existierende Content Provider zurückgreifen bzw. deren Inhalte in das eigene Programm integrieren.

Erfolgsfaktoren – Pflege der Inhalte

Das Curriculum und die Inhalte müssen regelmässig auf ihre Aktualität überprüft und bei Bedarf aktualisiert werden.

- Verantwortlichkeit einer bestimmten Person zuweisen
- in definierten Abständen einen Review einplanen (z.B. halbjährlich oder jährlich).

Auch andere Trigger sind möglich:

- Eine Sicherheitsrichtlinie wird hinzugefügt, geändert oder abgeschafft.
- Ein grösserer Vorfall tritt auf
- Eine wichtige neue Bedrohung wird entdeckt
- Es wird eine grössere Änderung technische oder organisatorische Änderung vorgenommen

Erfolgsfaktoren – Erfolgsprüfung I

Ein Security Awareness Programm darf nicht als eine einmalige Sache gesehen werden, die einfach gemacht wird, um eine bestimmte Anforderung zu erfüllen («*check in the box*»).

Ein effektives Training hat Ziele (warum wir es tun) und Ergebnisse (zu was werden die Teilnehmer befähigt, wenn sie daran teilgenommen haben).

- Die Ziele werden üblicherweise von Policies oder Direktiven abgeleitet und bestimmen wie das Ergebnisse aussehen soll, wie die Inhalte aufgebaut werden und welche Methoden eingesetzt werden.

- Wenn das Ziel beispielsweise darin besteht, die Häufigkeit erfolgreicher Phishing-Angriffe zu verringern, dann wäre ein anstrebenswertes Ergebnis, dass die Endnutzer in der Lage sind, Phishing-E-Mails zu identifizieren. Sowohl das Ziel als auch das Ergebnis sind messbar, was die Beantwortung der Frage "Funktioniert das?" erleichtert.

Erfolgsfaktoren – Erfolgsprüfung II

- Wir können also die Effektivität eines Security Awareness Trainings evaluieren, indem wir vor dem Training messen und danach. z.B. Vergleich der Anzahl erfolgreicher Phishings vor und nach dem Training.

- **Root Cause finden**: Bei der Bewertung der Wirksamkeit eines Schulungsprogramms ist es aber auf jeden Fall sehr wichtig, die Daten zu analysieren und keine voreiligen Schlüsse zu ziehen. Es könnte mehrere Gründe geben, warum ein Training nicht zu den gewünschten Ergebnissen führt. Evtl. werden die Phishing-E-Mails immer ausgeklügelter und schwerer erkennbar? Oder es ist dem Nutzer schlicht und einfach egal und er klickt weiterhin Links an und öffnet bedenkenlos Anhänge, solange es keine negativen Konsequenzen gibt.

Erfolgsfaktoren – Rolle der Geschäftsleitung I

- **Unterstützung der GL unabdingbar!**
  - Notwendige Ressourcen (personell wie finanziell)
  - Vorbildfunktion (Sensibilisierung der GL)

- **Motivation seitens GL**
  - Sicherheitsrisiken und die damit verbundenen Kosten
  - Auswirkung auf die Geschäftsprozesse
  - Gesetzliche Bestimmungen
  - Vorteile einer Zertifizierung (ISO 27001)
  - 'Best Practice' und Standards aus der Branche

Erfolgsfaktoren – Rolle der Geschäftsleitung II

Wie präsentiere ich überzeugend vor dem Management?

- Alle Unterlagen dabei, pünktlich, gut vorbereitet
- "Keep it simple and smart"
  - Klare nachvollziehbare Struktur
  - Einfach, verständlich, Sprache der Zielpersonen
  - So kurz wie möglich, so lang wie nötig
- Optionen aufzeigen, einfache Entscheidung ermöglichen
- Souveränes auftreten, angemessen gekleidet

Umgang mit Verstössen

- Verletzungen der Vorschriften zur Informationssicherheit können zu grossen Schäden führen.
- Sanktionen sind zu definieren und anzuwenden. Auch hier: Unterstützung des Managements notwendig.
- «Thema geht alle an», Verstösse melden.
- Das DS-GVO sieht bei Verstössen gegen den Datenschutz Geldbussen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes vor (dazu kommen Gerichtskosten sowie allenfalls Schadensersatzforderungen).

Agenda

1. The Human Factor – was ist das?
2. Warum Security Awareness Training?
3. Awareness Training planen und umsetzen
4. **Demo: Security Awareness Training Tool**

Demo KnowBe4

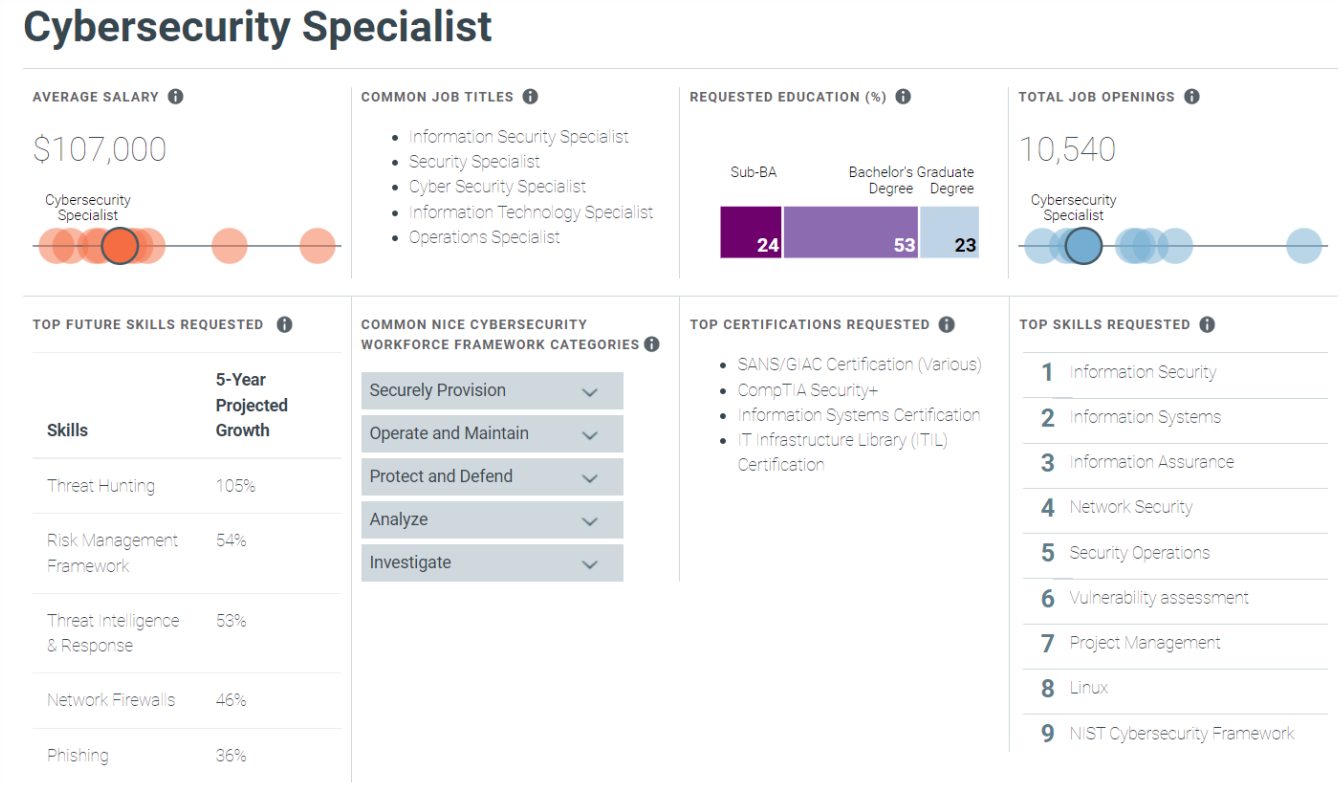
- Übersicht UI und Funktionalitäten
- Phishing
- Training
- Modstore/Bibliothek
- Reporting
- Phish Alert Button
- Smart Groups (Automatisierung)
- Eingliederung in sonstige Schulungsmassnahmen

Erfahrungen aus der Praxis

- Anforderungen des Kunden aufnehmen
- Onboarding und Initialkonfiguration
- Baseline Test und Umfragen
- Planung und Einrichtung von Kampagnen und anderen Aktivitäten
- Analyse und Reporting
- …

Vielen Dank für die Aufmerksamkeit!

Eine Karriere in Cyber Security



Cybersecurity Specialist

AVERAGE SALARY

$107,000

Cybersecurity Specialist

COMMON JOB TITLES

- Information Security Specialist
- Security Specialist
- Cyber Security Specialist
- Information Technology Specialist
- Operations Specialist

REQUESTED EDUCATION (%)

Sub-BA	Bachelor's Degree	Graduate Degree
24	53	23

TOTAL JOB OPENINGS

10,540

Cybersecurity Specialist

TOP FUTURE SKILLS REQUESTED

Skills	5-Year Projected Growth
Threat Hunting	105%
Risk Management Framework	54%
Threat Intelligence & Response	53%
Network Firewalls	46%
Phishing	36%

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Analyze
- Investigate

TOP CERTIFICATIONS REQUESTED

- SANS/GIAC Certification (Various)
- CompTIA Security+
- Information Systems Certification
- IT Infrastructure Library (ITIL) Certification

TOP SKILLS REQUESTED

1. Information Security
2. Information Systems
3. Information Assurance
4. Network Security
5. Security Operations
6. Vulnerability assessment
7. Project Management
8. Linux
9. NIST Cybersecurity Framework

https://www.cyberseek.org/pathway.html