

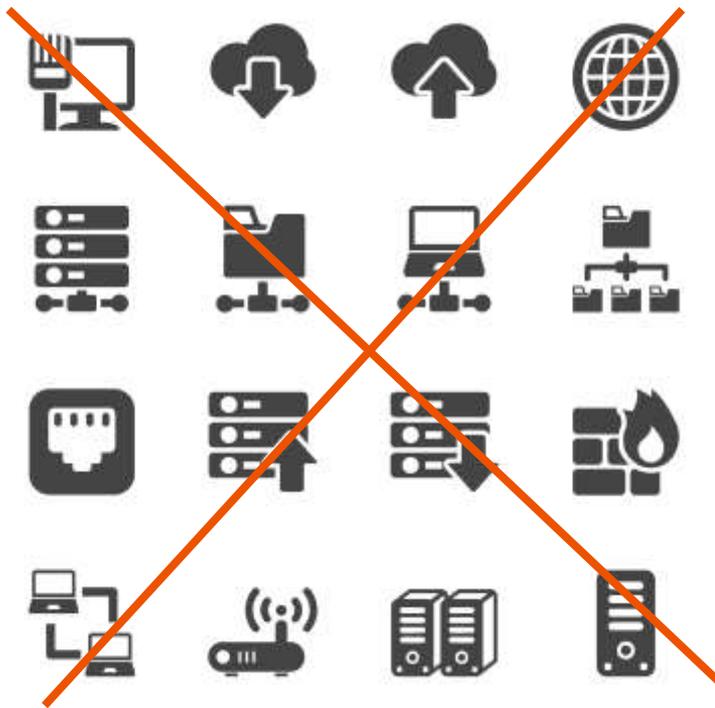
Security Awareness – **Zentraler Baustein für IT Sicherheit**

Nicolas Leiser
Geschäftsführung

| Cyber Samurai – Dienstleistungen für Ihre IT-Sicherheit



85 Prozent aller erfolgreichen Angriffe erfolgen über den Menschen und nicht über die Maschine



Mögliche Folgen eines Angriffs

Erpressung und Lösegeld	Unterbrechung des Betriebes	IT Wiederherstellungskosten	Management der Schadensbewältigung
IT-Forensik	Rechtsberatung	Fremdschäden	Vertragsstrafen und Bußgelder
Reputationskosten	Verbesserung der IT Security	Informationskosten	Krisenberatung
Krisenkommunikation	Litigation-PR	Nachhaltige Beseitigung des Reputationsschadens	 Bitkom Leitfaden



Ziele einer Security Awareness Kampagne

Die „menschliche Firewall“ aufbauen!

85% aller erfolgreichen Hackerangriffe basieren auf Social Engineering



- 1 Mitarbeiter vom Sicherheitsrisiko zum **aktiven Mitglied der Verteidigung** entwickeln.
- 2 **Begeisterung der Teilnehmer** für die Security Awareness Kampagne erwecken.
- 3 Individuell auf den Bedarf und die Fachrichtung jedes einzelnen Mitarbeiters **zugeschnittene Trainings + Phishing Simulationen**.
- 4 **Die akute Bedrohungslage aus dem Dark Web Monitoring** in der Kampagne reflektieren.
- 5 **KPI basierte Analyse** und Dokumentation des Mitarbeiterverhaltens (ISMS).
- 6 Kosten- und ressourcenschonendes Security Awareness Training -> **niedrige Total Cost of Ownership (TCO)**.

| Projektlauf – Vorbereitung



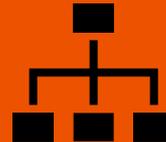
Anforderungs-
analyse



Kick-Off



Bereitstellung
und
Konfiguration
der Tools



Benutzer-
verwaltung

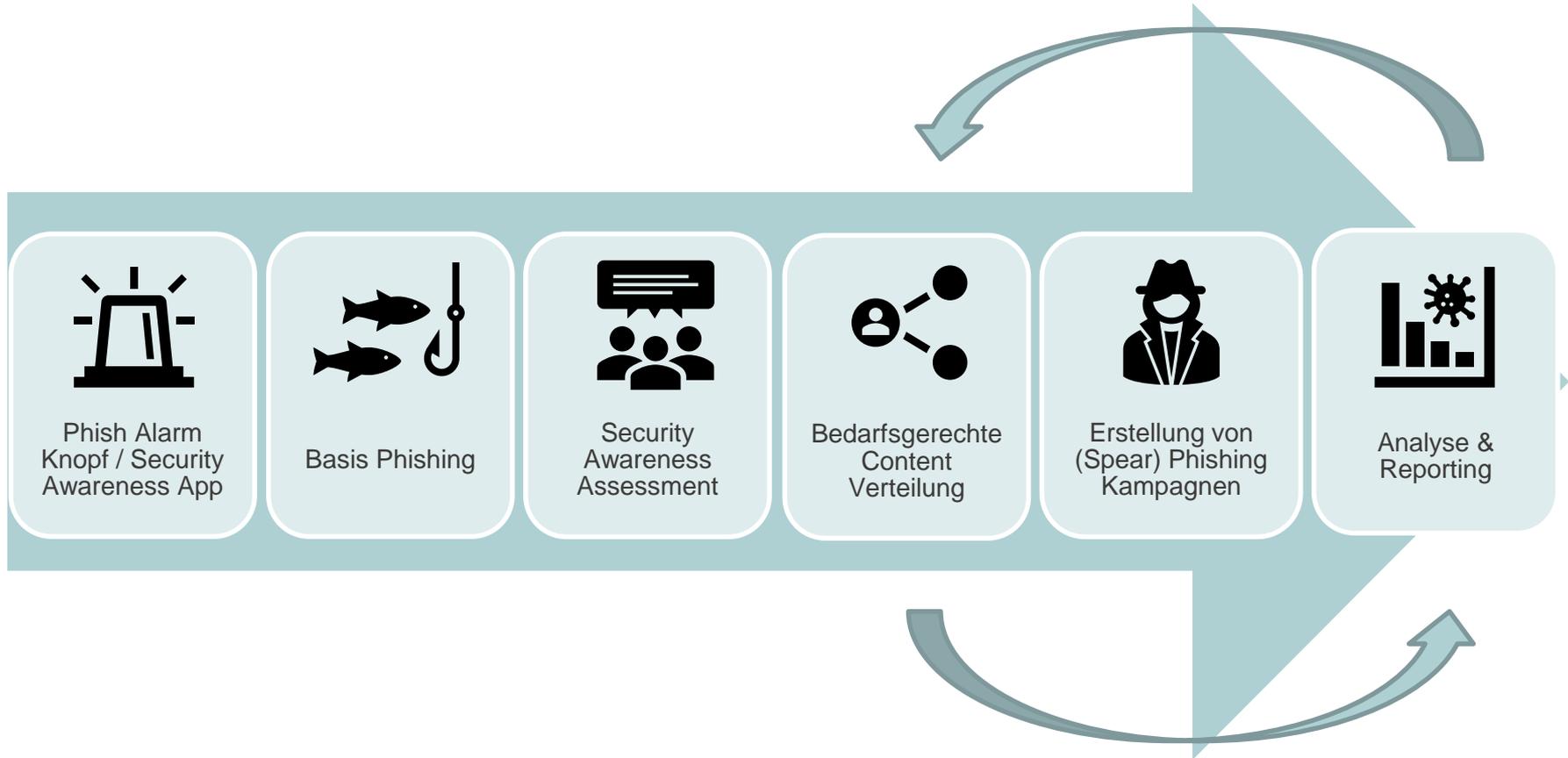


Whitelisting

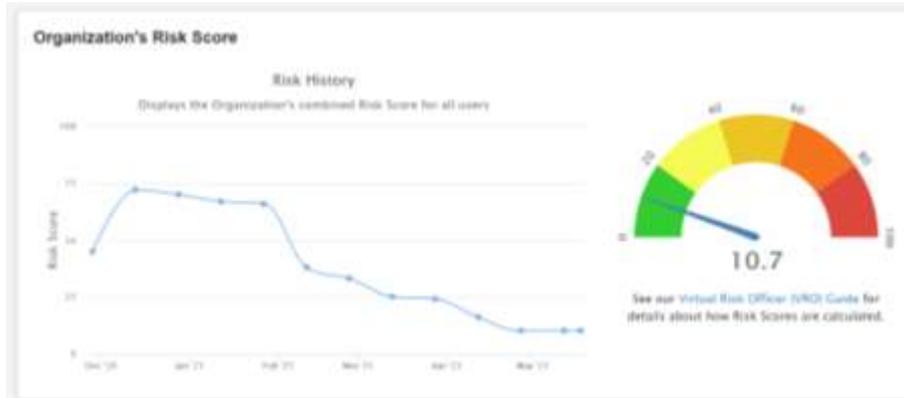


Mitarbeiter
Kommunikation

| Projektlauf – Durchführung



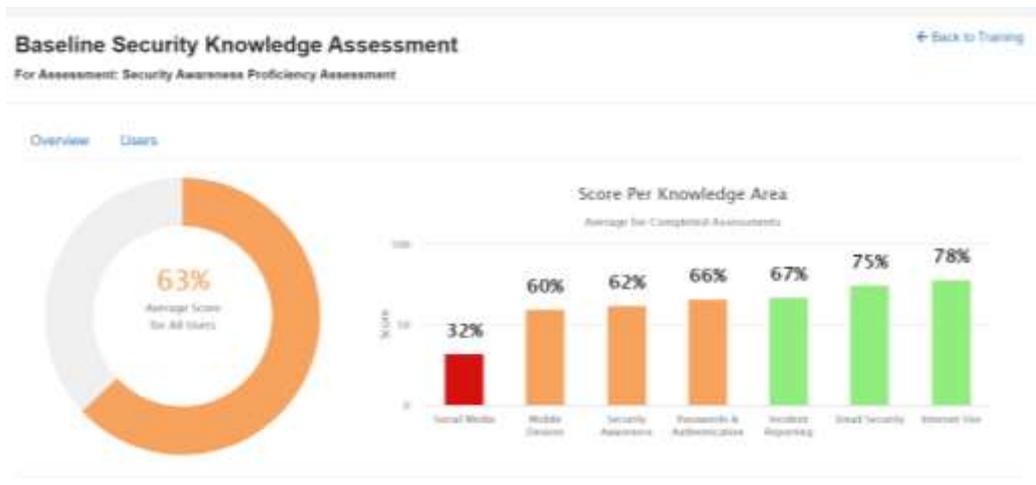
Reporting KPIs – Risk Score/Phishing Security Tests





Security Awareness Assessment – Kenntnisstand

Gezielt den Wissenstand ermitteln, um Trainings inhaltlich entsprechend zielgerichtet anzubieten.



Mitarbeiter bekommen **zielgerichtete Trainingsinhalte**, die ihre **Schwächen adressieren** und Wissen in den betreffenden Bereichen explizit auf-/ausbauen.

Condition: Must

Scope: Any Selected

Knowledge Area: Passwords & Authentication X

Comparison: Less Than

Score: 80

Time Frame: Most Recent Range Duration Any

Cancel Save



Relevante Trainingsinhalte ausrollen

Zielgerichtete Inhalte Assessments und dem Dark Web Monitoring basierend

Nach persönlichem Bedarf

Nach Dark Web Bedrohung

Nach Rolle/Funktion

Nach Region

Nach Branche

Training Campaigns				+ Create Training Campaign		
Campaigns				Notification Templates	Policies	Reports
Active		Inactive	All	Search		
Name	Groups	Content	Complete %			
In Progress Standard Training alle Mitarbeiter 11/05/2021 - 11/05/2021	Nur Nici not smart	<ul style="list-style-type: none">Security Awareness Proficiency AssessmentCEO Fraud - Fake PresidentClean Desk PolicyIndustrial EspionageRansomware Micro-module	<div><div></div></div>			
In Progress Facility Manager 11/05/2021 - 3 months	Nur Nici not smart	<ul style="list-style-type: none">Visitor Management	<div><div></div></div>			
In Progress Password Training vom Assessment 11/05/2021 - 3 months	Password Learner	<ul style="list-style-type: none">Secure Passwords With Quiz	<div><div>25%</div></div>			
In Progress Phishing alle Klicker 11/05/2021 - 3 months	Klickers	<ul style="list-style-type: none">Consent Phishing	<div><div></div></div>			
In Progress Baseline Training 18/03/2021 - 1 week	All Users	<ul style="list-style-type: none">Security Awareness Proficiency Assessment	<div><div>100% Completed</div></div>			



Vielfältige Security Awareness Trainingsinhalte

Ausrichtung nach thematischen Schwerpunkten um größtmögliche Relevanz zu schaffen.

Branche

- Finanzen, Gesundheit, Bau, Fertigung, Hotel und Gastgewerbe, Technologie, Dienstleistung etc.

Rolle

- Kundenservice, Entwickler, Management, Finanzen, IT, Marketing, Vertrieb etc.

Angriffsvektor

- (Spear) Phishing, Ransomware, Social Engineering, Tailgating, USB, Vishing etc.

Compliance

- GDPR bzw. internationale Compliance Standards

Human Resources

- Sicherheit am Arbeitsplatz, Mobbing, Ethik etc.

Häufige Themen

- Human Firewall, Social Media, Mobile Devices, Password and Authentication, Internet Use etc.



Beispiel: Phishing Mails und Landingpages

Phishing + Reaktion + Lerninhalte

Von: [REDACTED] Vorlagen-ID:29536-558756
Antwort an: [REDACTED]
Betreff: Zusammenarbeit [REDACTED] [Test-E-Mail an mich senden](#)
Projektskizze.pdf

< Sehr geehrter Herr [REDACTED] >

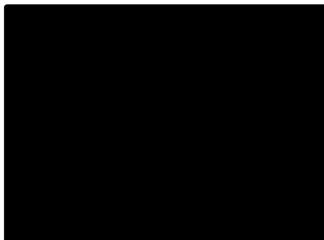
mit großem Interesse habe ich Ihren Artikel [REDACTED] gelesen und möchte Ihnen ganz herzlich für den Platz auf dem Siegertreppchen gratulieren.

[REDACTED] beschäftigt sich mit einem Thema, das vermutlich sehr nahe an Ihrem [REDACTED] liegt. Eine Zusammenarbeit könnte für alle Beteiligte sehr interessant sein.

Könnten Sie bitte anliegende Projektskizze einmal prüfen und bei Gefallen mit mir in Kontakt treten?

Sie erreichen mich am besten unter meiner Mobilnummer [REDACTED]

Mit freundlichen Grüßen



Von: [REDACTED] Vorlagen-ID:53238-908284
Antwort an: [REDACTED]
Betreff: [REDACTED] Alumni Artikel [Test-E-Mail an mich senden](#)

Externe Bilder anzeigen

Lieber [REDACTED]

wir würden gerne über Dich und Deiner erfolgreichen Gründung einen Artikel auf unserer Webseite im Alumni Bereich veröffentlichen.

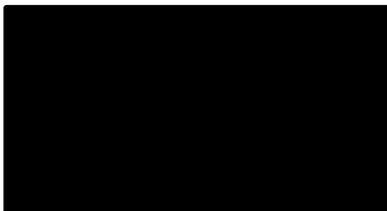
Wir haben dazu einen Entwurf erstellt, und würden Dich bitten diesen zu revidieren.

<https://www.frankfurt-school.de/home/about/alumni> [REDACTED]

Da der Artikel noch nicht öffentlich ist bitten wir Dich Benutzername T.Horn und Passwort Herbst2021! zu verwenden.

Für Rückfragen erreichst Du mich unter [REDACTED]

Beste Grüße,





CYBER SAMURAI

WE SERVE AND PROTECT

KONTAKT

Cyber Samurai GmbH
Brahmsstrasse 9
85591 Vaterstetten

Nicolas.Leiser@cyber-samurai.net
www.cyber-samurai.net