CloudCommand

Cyber Security

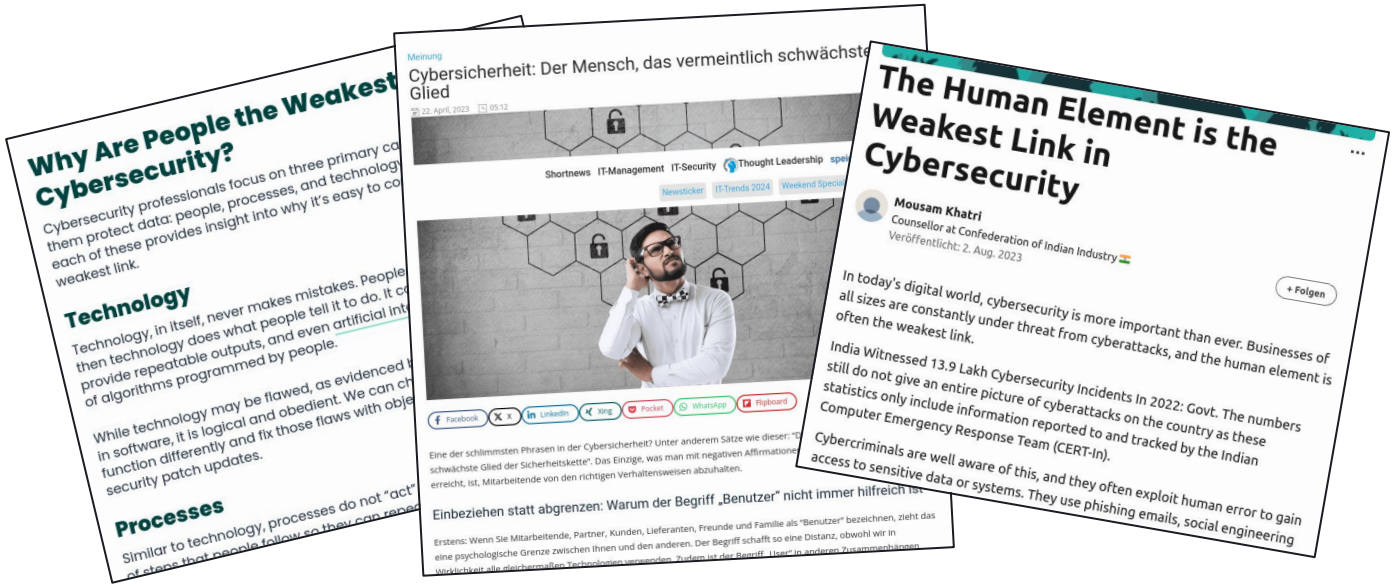
CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Schulung und Sensibili-sierung

Mitarbeiter als primäre Cyberangriffsfläche?



Methoden zur Sensibilisierung von Mitarbeitern

Bewusstsein für Bedrohungen schaffen:

- Schulungen helfen Mitarbeitern, aktuelle und potenzielle Netzwerksicherheitsbedrohungen wie Phishing, Malware, Ransomware und andere Cyberangriffe zu verstehen.

Richtlinien und Verfahren vermitteln:

- Mitarbeiter werden mit den Sicherheitsrichtlinien, -verfahren und Best Practices der Organisation vertraut gemacht, was zu einer stärkeren Compliance führt.

Methoden zur Sensibilisierung von Mitarbeitern

Förderung einer Sicherheitskultur:

- Regelmäßige Schulungen tragen dazu bei, eine Kultur der Sicherheit innerhalb der Organisation zu etablieren, bei der Sicherheit als gemeinsame Verantwortung angesehen wird.

Reaktion auf Vorfälle:

- Mitarbeiterschulungen umfassen oft Protokolle zur Reaktion auf Sicherheitsvorfälle, damit Mitarbeiter wissen, wie sie im Falle einer Sicherheitsverletzung reagieren sollen.

Methoden zur Sensibilisierung von Mitarbeitern

Umgang mit sensiblen Daten:

- Die Schulung betont die Bedeutung des Schutzes sensibler Daten und lehrt Methoden zur sicheren Handhabung und Speicherung von Informationen.

Physische Sicherheit:

- Schulungen decken auch Aspekte der physischen Sicherheit ab, wie den sicheren Umgang mit Hardware und den Zugang zu gesicherten Bereichen.

Methoden zur Sensibilisierung von Mitarbeitern

Aktualisierung des Wissens:

- Regelmäßige Schulungsprogramme stellen sicher, dass das Personal über die neuesten Sicherheitsbedrohungen und -technologien auf dem Laufenden bleibt.

Simulation von Sicherheitsvorfällen:

- Durch die Durchführung von simulierten Angriffen oder Sicherheitsübungen können Mitarbeiter praktische Erfahrungen im Umgang mit potenziellen Sicherheitsvorfällen sammeln.

Methoden zur Sensibilisierung von Mitarbeitern

Stärkung des Passwort-Managements:

- Schulungen betonen die Bedeutung starker Passwörter und lehren Best Practices für die Erstellung und Verwaltung von Passwörtern.

Sensibilisierungsthemen: Erkennung von Phishing

Ungewöhnliche Absenderadresse:

- Überprüfen, ob die E-Mail-Adresse des Absenders legitim ist. Oft sind Phishing-Mails von Adressen gesendet, die bekannten Unternehmen ähnlich sehen, aber geringfügige Abweichungen aufweisen, wie zusätzliche Buchstaben oder verdächtige Domains.

Dringlichkeit und Angstmacherei:

- Phishing-Mails enthalten oft dringende oder bedrohliche Nachrichten, die den Empfänger dazu bringen sollen, schnell zu handeln, ohne die Legitimität der E-Mail zu hinterfragen. Beispielsweise Warnungen vor Kontosperrung oder dringende Anfragen um vertrauliche Informationen.

Sensibilisierungsthemen: Erkennung von Phishing

Ungebetene Anhänge oder Links:

- Vorsicht mit E-Mails, die ungebetene Anhänge oder Links enthalten. Öffnen Sie keine Anhänge oder klicken Sie nicht auf Links, wenn Sie sich nicht sicher sind, dass die E-Mail vertrauenswürdig ist.

Rechtschreib- und Grammatikfehler:

- Phishing-E-Mails enthalten oft Rechtschreib- und Grammatikfehler. Professionelle Organisationen überprüfen ihre Kommunikation in der Regel sorgfältig, daher können solche Fehler ein Hinweis auf eine betrügerische E-Mail sein.

Sensibilisierungsthemen: Erkennung von Phishing

Aufforderung zur Eingabe persönlicher Informationen:

- Besondere Vorsicht ist geboten, wenn E-Mails dazu auffordern, persönliche oder finanzielle Informationen preiszugeben, wie Passwörter, Kontonummern oder Sozialversicherungsnummern. Legitime Unternehmen fordern solche Informationen normalerweise nicht per E-Mail an.

Sensibilisierungsthemen: Physische Sicherheit

Zugangskontrolle:

- Ausschließlich autorisiertes Personal sollte Zugang zu sensiblen oder gesicherten Bereichen erhalten. Die Nutzung von Sicherheitskarten, Codes oder biometrischen Systemen kann dabei helfen, den Zugang zu kontrollieren und zu überwachen.

Sicherer Umgang mit Besuchern:

- Besucher sollten immer registriert und während ihres Aufenthalts im Unternehmen begleitet werden. Dies verhindert unautorisierten Zugriff auf sensible Bereiche und schützt vertrauliche Informationen.

Sensibilisierungsthemen: Physische Sicherheit

Schutz sensibler Informationen:

- Wichtige Dokumente und Datenträger sollten sicher aufbewahrt werden, vorzugsweise in abgeschlossenen Schränken oder Räumen. Es sollte stets darauf geachtet werden, dass sensible Informationen nicht offen auf Schreibtischen oder in für jeden zugänglichen Bereichen liegen.

Bewusstsein für verdächtige Aktivitäten:

- Mitarbeiter sollten ermutigt werden, auf ungewöhnliche oder verdächtige Aktivitäten zu achten, wie unbekannte Personen in gesicherten Bereichen oder ungewöhnliche Anfragen nach Informationen oder Zugang.

Sensibilisierungsthemen: Physische Sicherheit

Sicherheitsbewusstes Verhalten:

- Die Wichtigkeit von sicherheitsbewusstem Verhalten, wie das Verriegeln von Türen, das sichere Verwahren von Schlüsseln oder Zugangskarten und das Ausschalten nicht genutzter Geräte, sollte betont werden. Dies trägt dazu bei, die physische Sicherheit im Unternehmen zu stärken.

Simulation

Realistische Szenarien:

- Entwickeln realistischer Szenarien, die auf tatsächlichen Sicherheitsrisiken basieren, denen die jeweilige Organisation ausgesetzt sein könnte. Dies kann von Phishing-Angriffen über Datenlecks bis hin zu physischen Sicherheitsverletzungen reichen.

Einbindung sämtlicher Ebenen:

- Sicherheitssimulationen sollten Mitarbeiter aller Ebenen einbeziehen, von der Geschäftsführung bis hin zu den operativen Teams. Jeder sollte verstehen, wie er auf verschiedene Arten von Sicherheitsvorfällen reagieren muss.

Simulation

Debriefing und Feedback:

- Nach jeder Simulation ist ein Debriefing entscheidend. Hierbei handelt es sich um eine Besprechung der Simulation, um zukünftige Trainings und Sicherheitsprotokolle zu verbessern.

Klare Kommunikation:

- Allgemein ist es stets wichtig, sicherzustellen, dass alle Beteiligten verstehen, dass es sich um eine Simulation handelt, um unnötigen Alarm oder Verwirrung zu vermeiden. Gleichzeitig sollte die Kommunikation während der Simulation realistisch gehalten werden, um eine echte Notfallsituation zu simulieren.

Simulation

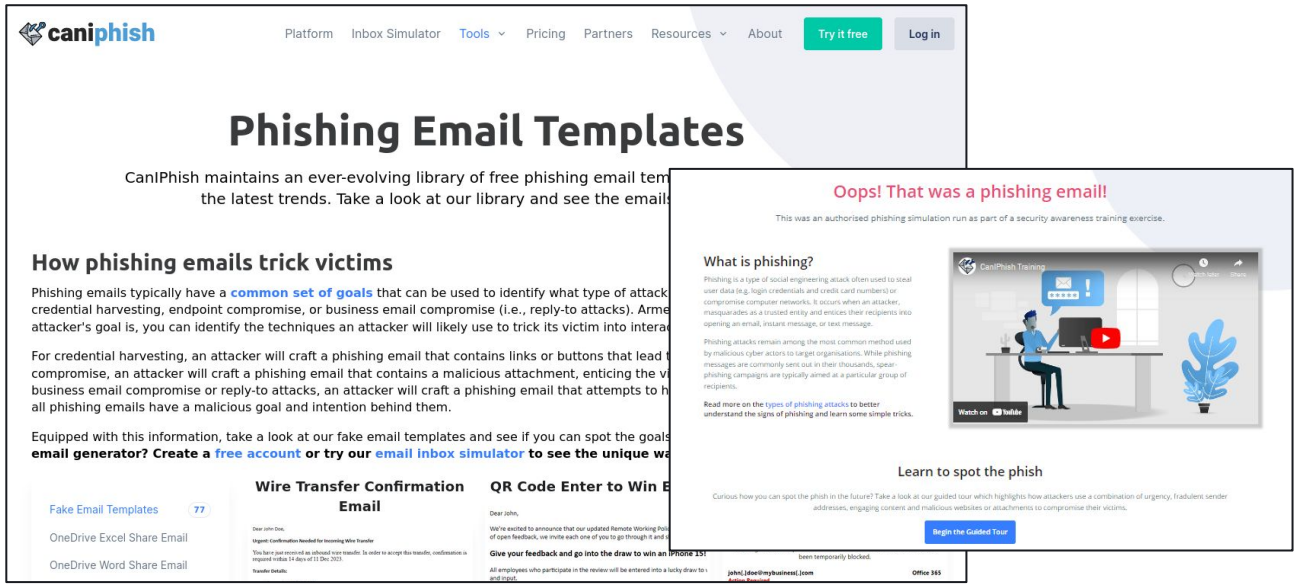
Regelmäßige Durchführung und Aktualisierung:

- Sicherheitssimulationen sollten regelmäßig durchgeführt und ihre Szenarien aktualisiert werden, um mit den sich ändernden Sicherheitsbedrohungen Schritt zu halten. Dies stellt sicher, dass das Personal stets auf dem neuesten Stand ist und sich der besten Reaktionspraktiken bewusst ist.

Tools: CanIPhish

CanIPhish ist ein Tool, welches vorgefertigte Vorlagen für Phishing-E-Mails bereitstellt, um das Sicherheitsbewusstsein der eigenen Belegschaft zu testen. Statt eines tatsächlichen Angriffs wird das Opfer zu einer Seite geleitet, die es auf seinen Fehler aufmerksam macht.

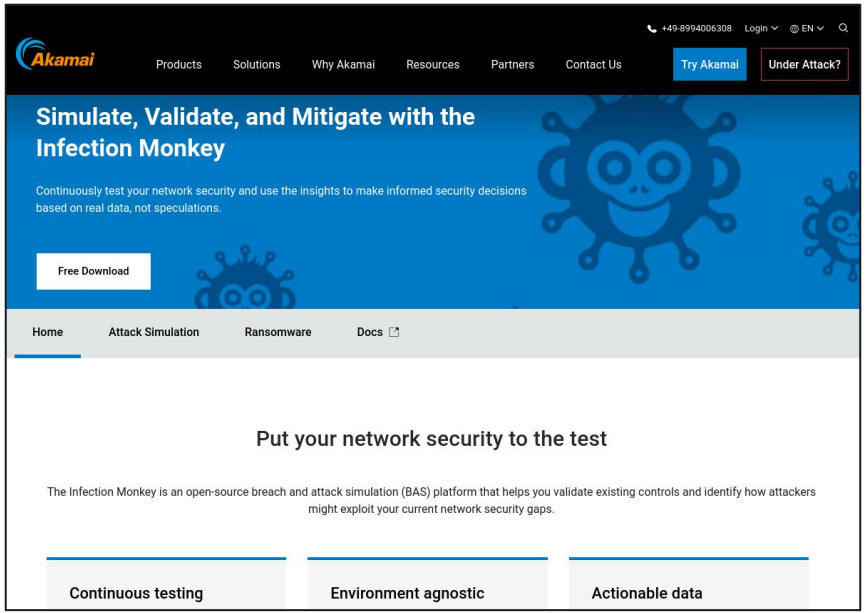
Tools: CanIPhish



Tools: Infection Monkey

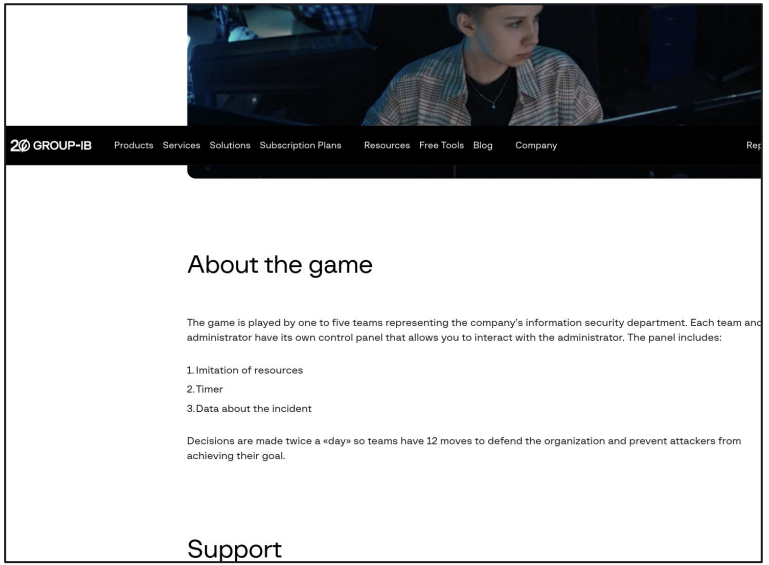
Infection Monkey ist eine Open-Source Simulationsplattform für verschiedene Angriffe auf Netzwerke mit anschließender Auswertung und Verbesserungs-vorschlägen.

Tools: Infection Monkey



Tools: Spielerische Simulationsprogramme

Verschiedene Firmen wie etwa Group-IB bieten spielerische Simulationstrainings, welches Mitarbeiter auf unterhaltsame Weise die Wichtigkeit von IT-Sicherheitsbewusstsein vor Augen führen.



CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm