
Zu Hause in Erfurt. KOWO
12.500
Wohnungen
660.000 m²
Wohnfläche
206
Mitarbeiter
IT
5
IT- Mitarbeiter
Erfahrungsbericht zu unserem Umgang
mit der Informationssicherheit zum WZT2024

2022 haben wir im Zuge einer Umstellung der IT-Struktur eine Bestandsaufnahme durchgeführt

Was war gut?

- Wir haben einen guten IT-Dienstleister mit hoher Priorität auf Sicherheit
  (ISO 27001 Zertifiziert)

IBYKUS

- Wir haben eine jährliche formale Datenschutzschulung

Was war nicht so gut?

- Viele Mitarbeiter interessierten sich nicht für Informationssicherheit
  - Rechner wurden beim Verlassen nicht gesperrt
  - Mentalität: „IT-Sicherheit macht bei uns die IT“
- Dass wir vieles nicht wussten

Erste Versuche unsere Lücken zu identifizieren

Konfrontation unserer Mitarbeiter wegen ungesperrten Rechnern

- Negatives Feedback und Unverständnis

Teilnahme an Phishing-Simulation des VTW mit Trainstitute

- Durchschnitt 5,9% Klickrate
  (13,6% bei spezifischer E-Mail)
- Erkenntnisse zum Risikofaktor „Mitarbeiter“ in Zahlen

Vorbereitung einer Informationskampagne

Zusammenarbeit mit einem Partner für Informationssicherheit

CANCOM

- Beratung
- Pentest

Anschaffung einer Awareness Plattform zur Informationssicherheit

KnowBe4

- Phishingtests in Eigenorganisation
- Schulungsvideos zur Awareness - Informationssicherheit

Durchführung einer Informationskampagne (Einbezug des BR)

Konfrontation unserer Mitarbeiter wegen ungesperrten Rechnern
- Mit dem Ziel des Verständnisses

Einführung einer zwingenden aber guten Schulung
über die KnowBe4 Plattform zur Informationssicherheit (je Quartal)

Einführung eines Meldebuttons im Outlook für Phishingverdacht

Regelmäßige Aufklärung über Angriffe zu Betriebsversammlungen
- Berichte über erfolgreiche Angriffe auf bekannte Unternehmen
- Darstellung und Erklärungen zu Angriffen auf unser Unternehmen

Pentest der CANCOM

Sehr gute Überprüfung der Infrastruktur

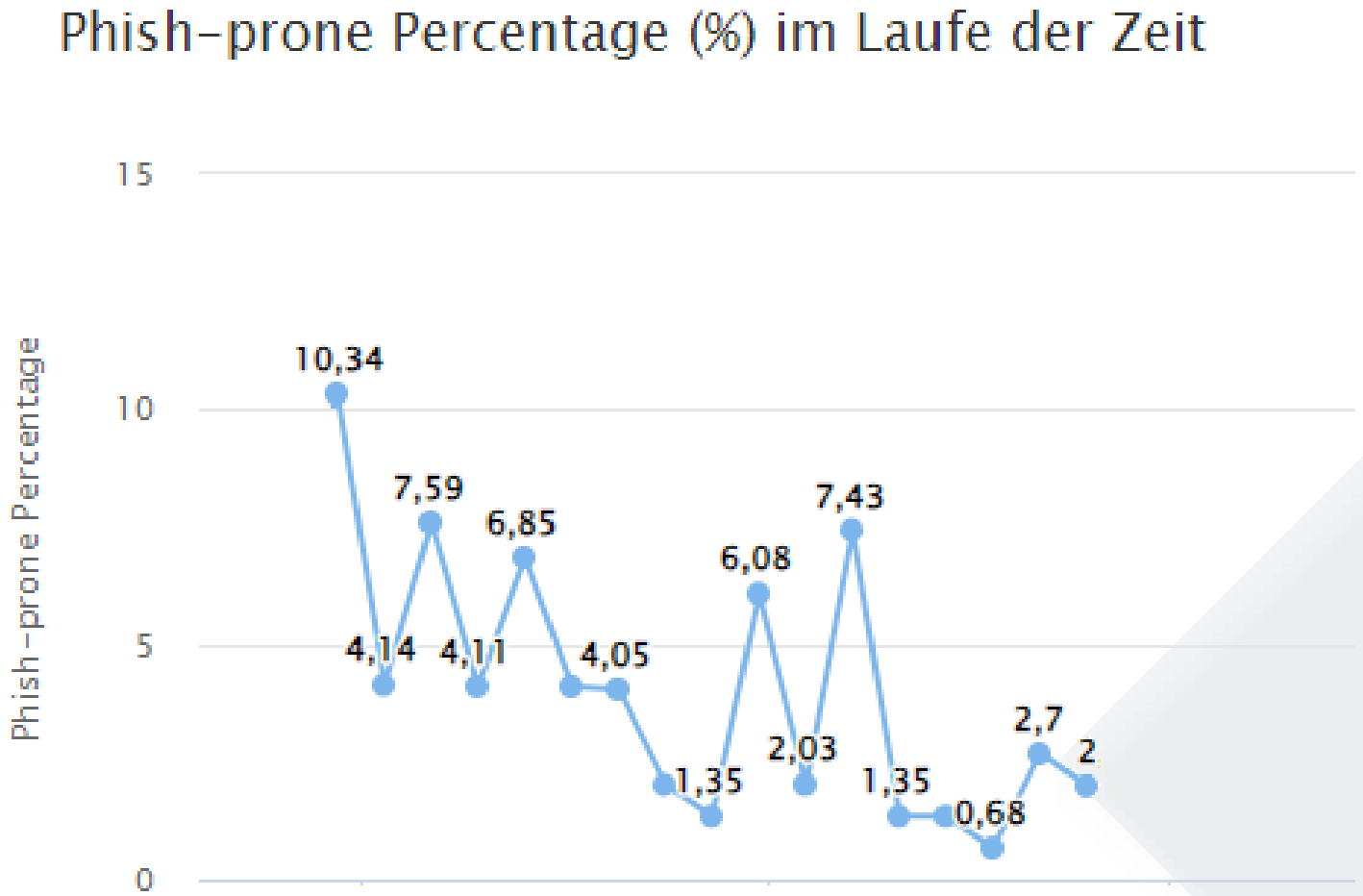
- Führte zu guten Erkenntnissen und Anpassungen bei unserem IT-Dienstleister

10% der Mitarbeiterpasswörter des AD wurden „erraten“

- „A-Ha-Effekte“ im Haus

Strukturierte Phishingtests aus der Knowbe4 Plattform

Jeder Mitarbeiter bekommt wöchentlich eine E-Mail aus einem Pool aus 50 E-Mails



Ergebnisse:

Die Mitarbeiter fühlen sich mitgenommen,
sind sich der Situation bewusst und verstehen,
dass sie Teil der Informationssicherheit sind

- Hohe Anzahl gemeldeter E-Mails (viele true positive -Meldungen)
- Umsetzung von „only share nacessary“ erkennbar

Wir behalten die Awareness aufrecht

- Quartalsweise „Schulungen“
- Anhaltende Phishingtests
- Fester IT TOP in Betriebsversammlung

Freigabe zur Wiederholung Pentest mit Elementen des Socialengineering

Projekt zur Einführung einer MFA-Lösung

Einsatz ist bisher (scheinbar) erfolgreich

Vielen Dank für die Aufmerksamkeit sagt die

KOWO

Ebenfalls Dank für die Unterstützung
und Zusammenarbeit an

CANCOM

KnowBe4

IBYKUS

TRAINSTITUTE

und an alle KoWo Mitarbeiter

Patrick Ziegler
IT-Management
KoWo mbh Erfurt
Patrick.Ziegler@KoWo.de