



CYBERDISE

Basierend auf den neuesten wissenschaftlichen Erkenntnissen über KI und menschliches Verhalten

Eine weitere CYBERDISE Lösung – implementiert bei:



GLB Gruppe – Mit CYBERDISE Awareness zur nachhaltigen Sicherheitskultur



AUF EINEN BLICK

Branche

Bauunternehmung

Herausforderung

Schutz von Handwerkerinnen, von Bauleuten, Anlagen und Daten vor den Risiken durch Cyberkriminelle.

Lösung

- CYBERDISE Business Edition.
- Regelmässige, dem Arbeitskontext angepasste Schulungen und Phishing-Kampagnen.

Vorteile

- Man fand eine unkomplizierte und intuitive Lösung mittels CYBERDISE.
- Kompatibilität mit bestehender IT-Infrastruktur.
- LMS für Drittkurse nutzbar.
- KI vereinfacht die Arbeit.
- Vielfältige Auswahlmöglichkeiten der CYBERDISE Software.
- Effektiver Schutz durch erwiesenen besser sensibilisierte und befähigte Mitarbeitende.

DIE GLB Gruppe

Die GLB Gruppe mit Hauptsitz in Langnau im Emmental ist eine führende Anbieterin für Bau-, Holzbau- und Immobilien-Dienstleistungen in der Schweiz. Sie vereint unter ihrem Dach Handwerkskunst, Planungskompetenz und moderne Bauausführung. Mit über 1.100 Mitarbeitenden an zahlreichen Standorten bedient die GLB sowohl private als auch gewerbliche Kunden. Die Unternehmensgruppe steht für regionale Verankerung, Qualität und Nachhaltigkeit.

HERAUSFORDERUNG

„Wir haben bei der GLB Gruppe im Bereich IT-Sicherheit umfassende Massnahmen getroffen – Firewalls, rasches Patching, End-point-Schutz und vieles mehr – doch der Mensch bleibt das zentrale Einfallstor für Cyberangriffe“, sagt Ismael Aemisegger, Leiter IT-Support bei der GLB Gruppe.

Gemäss einer IBM-Studie aus dem Jahr 2024 begannen über 47 % der erfolgreichen Cyberangriffe beim

Mitarbeiter. Gleichzeitig stieg die durchschnittliche Schadenssumme in den letzten fünf Jahren um 20 % auf 4,88 Millionen US-Dollar an.

Ein besonderes Problem: Die Belegschaft der GLB besteht primär aus Handwerkern, die nicht regelmäßig am PC arbeiten. Herkömmliche Phishing-Simulationen, wie sie für Dienstleistungsunternehmen erstellt wurden, greifen hier zu kurz. Sie adressieren Zielgruppen mit täglichem E-Mail-Verkehr – ein Umfeld, das für viele Mitarbeitende auf der Baustelle nicht repräsentativ ist.

LÖSUNG

Diese Herausforderung hat die GLB Gruppe früh erkannt. „Um unsere Mitarbeitenden kontinuierlich zu schulen und ihr Sicherheitsbewusstsein zu stärken, setzen wir auf CYBERDISE Awareness“, so Ismael Aemisegger.

Die Plattform von CYBERDISE ermöglicht es der GLB, ein massgeschneidertes Sensibilisierungsprogramm durchzuführen. Dieses umfasst gezielte, teilweise individu-



Interne Analysen zeigen, dass Awareness-Programme von CYBERDISE das Sicherheitsniveau eines Unternehmens signifikant erhöhen. Dies wurde auch bei der GLB rasch sichtbar – ein klarer Beleg für die Wirksamkeit der Plattform.

«Beeindruckend ist das mit Hilfe von KI gesteigerte Sensibilisierungsniveau. Diejenigen GLB Mitarbeiter, welche mit durch die KI individualisierten Phishingsimulationen konfrontiert wurden, zeigten bei der Nachmessung eine +50% bessere Sensibilisierung.»

ell erstellte Schulungen, lokalisierte Phishing-Simulationen verschiedener Schwierigkeitsstufen und natürlich eine strukturierte Auswertung der Ergebnisse. CYBERDISE Awareness wurde auch mit Microsoft Azure Apps und AD verbunden. Weiter wurde das interne Team im Produkt geschult.

VORTEILE

Besonders überzeugt zeigte sich die GLB von der intuitiven Bedienbarkeit der CYBERDISE-Lösung. Dank der individuellen Anpassungsfähigkeiten und der Möglichkeit, Vorlagen zu lokalisieren konnten Kampagnen schnell und effektiv aufgesetzt werden.

Ein breites Spektrum an Lernmodulen – von interaktiven Kursen über Videos bis hin zu Simulationen – ermöglicht ein abwechslungsreiches und praxisnahes Lernen. Weiter ist CYBERDISE Awareness auf höchsten Datenschutz und Datensicherheit ausgelegt. Die Lösung

ist vollständig DSGVO / DSGVO-konform, bietet starke Verschlüsselung auf Applikations- und Datenbankebene und setzt standardmässig auf anonymisierte Datenerhebung, ohne dass der Sensibilisierung-Rating des Einzelnen verloren geht.

ERGEBNIS

„Schon die ersten Ergebnisse haben uns gezeigt, wie wirkungsvoll die Massnahmen sind: Mitarbeitende, die mit einer simulierten Phishing-Mail bedient sind, haben ihr Verhalten nachweislich geändert. Das Bewusstsein für IT-Sicherheit ist deutlich gestiegen“, fasst Ismael Aemisegger zusammen.

Die Wirkung der Massnahmen zeigte sich in einem kontinuierlichen Anstieg der Aufmerksamkeit und Sensibilität der Mitarbeitenden. Besonders effektiv erwiesen sich dabei die realitätsnah gestalteten und vor allem die mit Hilfe der KI generierten Phishing-Kampagnen.

„Die wachsende Bedrohungslage durch gezielte Angriffe bestärkt uns, weiterhin in die Security Awareness unserer Mitarbeitenden zu investieren“, sagt Ismael Aemisegger.

Damit ist die GLB Gruppe auf einem guten Weg, eine gelebte Sicherheitskultur im Unternehmen zu etablieren – als nachhaltiger Schutz vor Cyberrisiken.



[cyberdise-awareness.com /download](https://cyberdise-awareness.com/download)

Cyberdise AG, Poststrasse 26, CH-6300 Zug, Switzerland, +41 44 551 78 10
backoffice@cyberdise.io | support@cyberdise.io