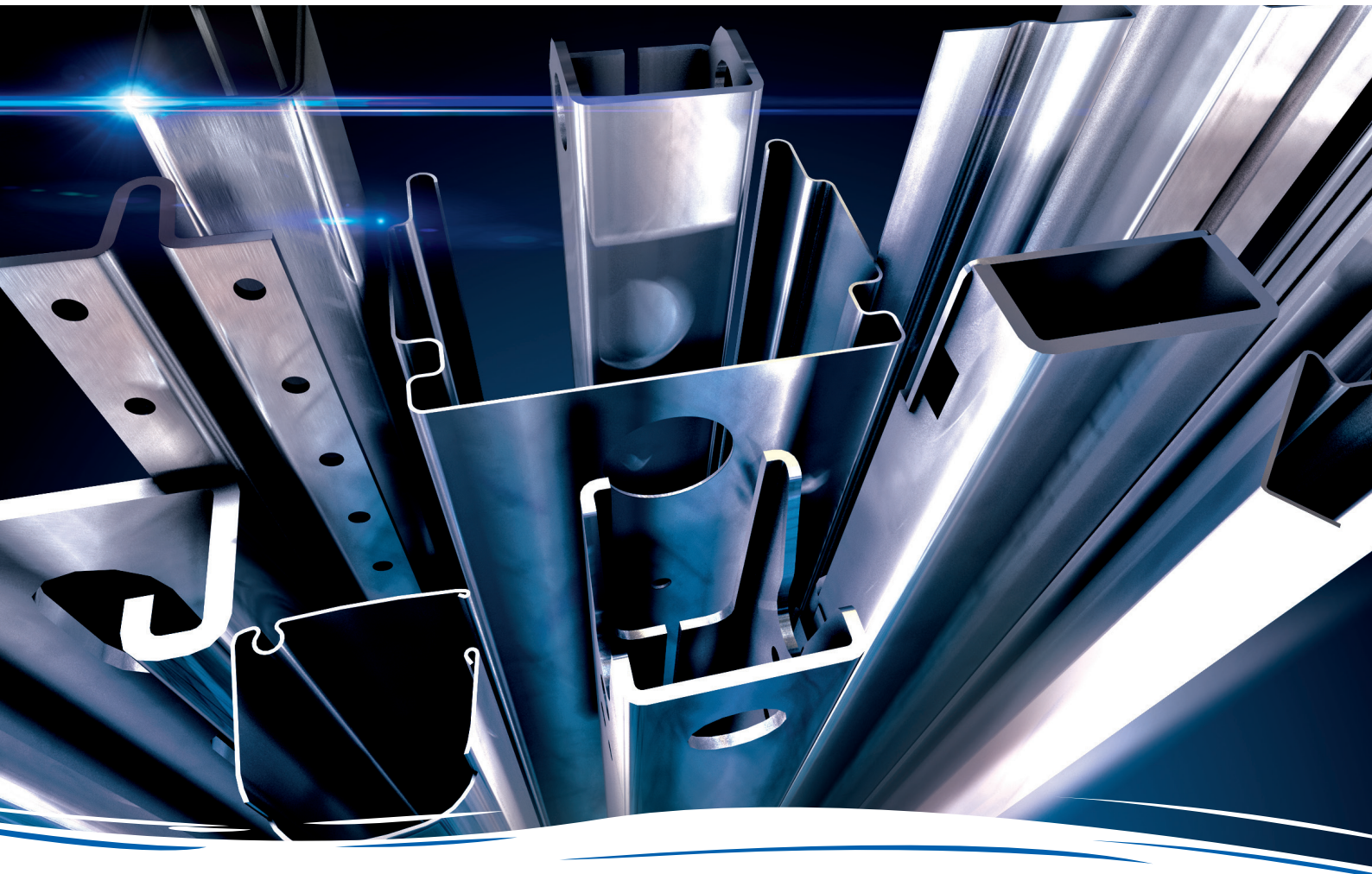


Customer Success

KIRCHHOFF ●●●
& LEHR ●●
METALL IN BESTFORM ●●



Der Hintergrund

Phishing-Angriffe können einen Herstellerbetrieb empfindlich treffen und sogar die gesamte Produktion lahmlegen. Entgangene Gewinne sind die Folge, außerdem schwindet das Kundenvertrauen und die Wettbewerbsfähigkeit sinkt.

Kirchhoff & Lehr, europaweit bekannter Spezialist für Profilertechnik, kann sich solche Ausfälle nicht leisten. Mit über 110 Mitarbeitern stellt das Unternehmen am Standort Arnsdorf kaltgewalzte Profile für zahlreiche Einsatzgebiete her, darunter die Automobilindustrie, Elektrotechnik, Sanitär, Torsysteme und Trockenbau. Neben diesem breiten Produktspektrum hat sich Kirchhoff & Lehr durch einen hohen Qualitätsstandard, Liefertreue, Preiswürdigkeit und exakt auf die Kundenanforderungen zugeschnittene Profile einen Namen gemacht. Das zeigt sich auch an der IATF-Zertifizierung, die dem Unternehmen als Automobilzulieferer ein hohes Qualitätsniveau attestiert.



Robert Batz
Leitung IT - Kirchhoff & Lehr GmbH

Die Herausforderung

Obwohl Kirchhoff & Lehr - wie viele andere Unternehmen - auch vorher schon mit Phishing konfrontiert war, wuchs die Zahl der gefälschten E-Mails während der Corona-Krise sprunghaft an. So nutzten viele Cyberkriminelle die Angst vor dem Virus, um ihre Opfer zum Öffnen von schadhaften Links oder Anhängen zu verleiten. Andere wiederum lockten die Nutzer auf nachgestellte Webseiten, um dort ihre Log-in-Daten abzugreifen.

„Mit der Masse an täglichen (Spear)-Phishing-Mails stieg die Gefahr, dass nicht alle von der IT-Abteilung abgefangen werden können, sondern sämtliche IT-Schutzmechanismen durchbrechen“, erinnert sich Robert Batz, Leiter IT bei Kirchhoff & Lehr. „Daher suchten wir nach externer Unterstützung, um die Belegschaft für Phishing-Angriffe und die IT-Sicherheit zu sensibilisieren.“

Die Lösung



Nach einem einmonatigen Testlauf mit den Security-Awareness-Trainings von IT-Seal stand für die Verantwortlichen fest: Diese Schulungen sollen zu einer Dauereinrichtung für die Beschäftigten in der Verwaltung werden. Das liegt vor allem an den Spear-Phishing-Simulationen, die einen hohen pädagogischen und didaktischen Nutzen bieten.

Informationskampagne für Mitarbeiter

Bevor die Awareness-Trainings starteten, wurden die Mitarbeiter entsprechend den Datenschutzregelungen darüber eingehend informiert und um ihre Einwilligung gebeten. „Dann wählten wir in enger Zusammenarbeit mit IT-Seal geeignete Phishing-Szenarien aus, um die Trainings-Mails gezielt auf die einzelnen Verwaltungsmitarbeiter zuschneiden zu können“, berichtet IT-Leiter Robert Batz. Das Organigramm von Kirchhoff & Lehr leistete wertvolle Unterstützung, da es die Beziehungen zwischen und in den Abteilungen abbildet.

„Wir haben zur Phishing-Simulation ein überwältigendes Feedback erhalten“

Robert Batz - Leitung IT - Kirchhoff & Lehr GmbH

Phishing-Simulationen und Meldebutton

Seit Anfang 2022 sendet IT-Seal den Beschäftigten regelmäßig nachgestellte Spear-Phishing-Mails, die angeblich von ihren Vorgesetzten, Mitarbeitern, Kollegen oder externen Stellen stammen. Fällt ein Mitarbeiter auf einen simulierten Phishing-Angriff herein, landet er direkt auf einer interaktiven Erklärseite, die ihm Hinweise auf verdächtige Merkmale gibt: ob Buchstabendreher in der Adresszeile, gefälschte Subdomains oder zweifelhafte Links. Über die Lernplattform „Security Hub“ stellt IT-Seal den Beschäftigten ergänzende E-Learnings zur Verfügung.

Zusätzlich wird das Sicherheitsbewusstsein der Beschäftigten durch den direkt in Microsoft Outlook integrierten IT-Seal Reporter Button geschult. Ist sich ein Nutzer unsicher, ob eine empfangene E-Mail gefälscht ist, kann er diese per Knopfdruck zur technischen Prüfung an die IT-Abteilung weiterleiten. Je nachdem wird die Mail dort gesperrt oder freigegeben.



Erfolgreiches Awareness-Training

Große Lernfortschritte messbar

Schon nach wenigen Monaten zeichnen sich große Lernfortschritte der Mitarbeiterinnen und Mitarbeiter in der Erkennung von Spear-Phishing-Angriffen ab. Messen lassen sich diese mit dem patentierten Employee Security Index (ESI®) von IT-Seal. Er bietet eine Kennzahl zur Ermittlung des Sicherheitsverhaltens der Mitarbeiter und wird danach berechnet, wie diese auf simulierte Phishing-Mails unterschiedlicher Schwierigkeitsgrade reagieren. Verschlechtert sich der ESI®, steuert die KI-gestützte Awareness Engine von IT-Seal automatisch nach und passt Zahl und Schwierigkeitsgrade den individuellen Lernbedarfen an.

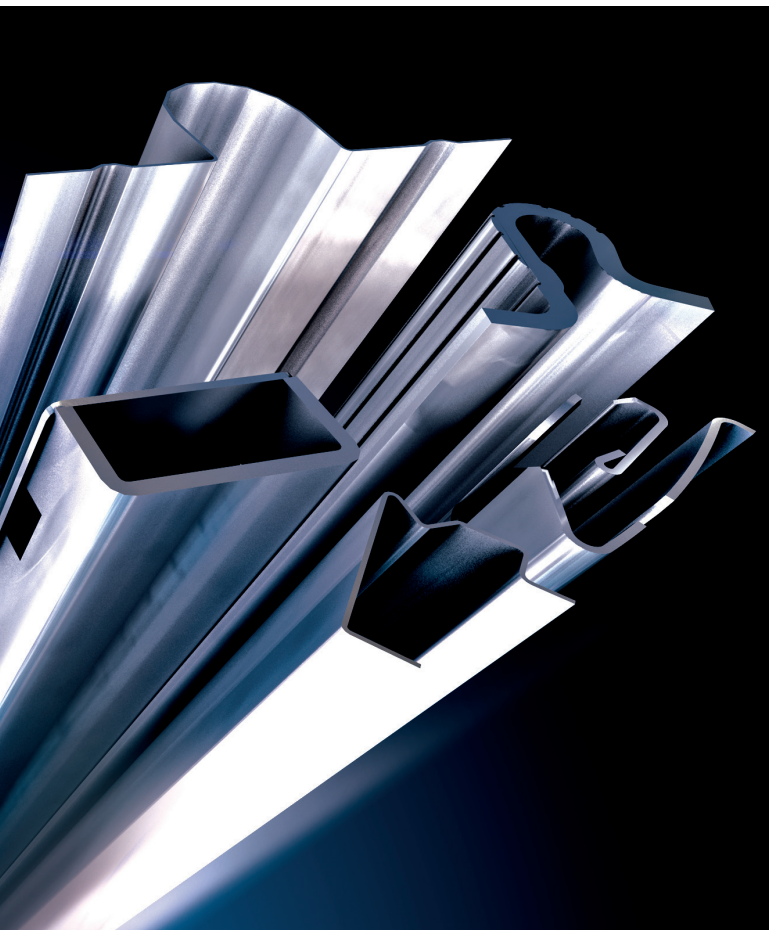
Über ein Management Dashboard kann IT-Chef Robert Batz die ESI®-Entwicklung in den einzelnen Abteilungen und Gruppen jederzeit anonymisiert einsehen. So kann er die aktuellen Lernfortschritte kontrollieren und erhält eine Grundlage für die weitere Kampagnenplanung mit IT-Seal.



Laufende Fortführung geplant

Bereits heute weist diese Planung weit über die ursprünglich vereinbarte Vertragslaufzeit hinaus, damit die Beschäftigten „in Übung“ bleiben und auch neue Mitarbeiter in das Training eingebunden werden können. Zudem ist eine Erweiterung des IT-Seal-Angebots um Vishing-Awareness-Trainings vorgesehen, bei denen die Mitarbeiter simulierte Angriffe mit Hilfe des Telefons erleben. Sie werden dabei aufgefordert, Informationen preiszugeben oder schädliche Handlungen auszuführen. Lässt sich ein Angerufener dazu verleiten, unterbricht IT-Seal den simulierten Angriff und löst die Situation auf. So wird erreicht, dass die Mitarbeiter sicherer im Umgang mit Vishing-Attacken im Tagesgeschäft werden.

IT-Leiter Robert Batz ist sich sicher, dass sich die Beschäftigten auch für diese Trainings begeistern werden: „Wir haben zur Phishing-Simulation ein überwältigendes Feedback erhalten, unsere Mitarbeiter haben die wachsenden Phishing-Gefahren und ihre eigene Verantwortung als menschliche Firewall erkannt.“ Er selbst schätzt neben den guten Inhalten, Methoden und Werkzeugen des IT-Seal-Angebots vor allem den angenehmen und kompetenten Umgang mit der Kundenbetreuerin. „Unsere Ansprechpartnerin bei IT-Seal hat immer ein offenes Ohr für unsere Anliegen und Vorschläge und ist immer für uns erreichbar. So ist im Laufe unserer Zusammenarbeit ein freundschaftliches Verhältnis entstanden, das dem Aufbau einer nachhaltigen Sicherheitskultur bei Kirchhoff & Lehr mehr als zugutekommt.“



Fazit

„Das Feedback unserer Mitarbeiter auf die Spear-Phishing-Simulationen von IT-Seal ist überwältigend. Sie werden systematisch für die wachsenden Phishing-Gefahren sensibilisiert und machen sich die große Verantwortung bewusst, die sie als menschliche Firewall zur Abwehr der zunehmenden Phishing-Attacken tragen.“

Robert Batz - Leiter IT bei Kirchoff & Lehr GmbH

Security-Awareness-Trainings von IT-Seal: Vorteile auf einen Blick

- ✓ Spear-Phishing-Simulationen trainieren Angriffserkennung
- ✓ E-Learnings, Online- und Präsenz-Seminare vertiefen Lerninhalte
- ✓ Employee Security Index (ESI®) macht Sicherheitsbewusstsein messbar
- ✓ Reporter Button unterstützt Identifizierung zweifelhafter E-Mails
- ✓ Management Dashboard für zeitnahe Kontrolle der Lernfortschritte
- ✓ Security Hub bietet Mitarbeitern individuelle Lernplattform
- ✓ Kampagnen immer auf neuestem Angreifer-Stand
- ✓ Full-Service-Angebot entlastet interne Ressourcen



Über Kirchhoff & Lehr GmbH

Kirchhoff & Lehr GmbH



Kirchhoff & Lehr ist ein europaweit bekannter Hersteller von kaltgewalzten Profilen. Das Spektrum reicht von einfachen Standardprofilen über Spezialprofile bis hin zu komplexen Systemen. Mit 110 Mitarbeitern am Standort Arnsdorf gehört das Unternehmen zur Tillmann Gruppe, einem Verbund aus drei weiteren eigenständigen Unternehmen. Als Hersteller in der Metallverarbeitungsbranche beliefert Kirchhoff & Lehr Kunden in Automobilindustrie, Elektrotechnik, Sanitär, Torsystemen und Trockenbau.

www.tillmann-gruppe.de

