SHD.
WIR BEWEGEN IT.

IT-Sicherheit

User Awareness

Nutzersensibilisierung als Workshop oder „as a Service“

Mehr als 70 % aller Angriffe auf die IT-Sicherheit setzen die Interaktion von Mitarbeitenden voraus. Umso wichtiger ist die Ansprache aller Unternehmensvertreter zur Umsetzung von IT-Security.

Informierte und achtsame Kolleginnen und Kollegen bilden einen effektiven Schutz gegen Angriffe, wenn sie über gängige Angriffsmethoden aufgeklärt wurden und bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen.

LÖSUNG #1

Awareness-Schulung vor Ort

Im Rahmen unseres Workshops erfahren Ihre Mitarbeitenden, welche Gefahren im Internet lauern, was Social Engineering ist und wie sie auf Vorfälle reagieren können. Ziel der Sensibilisierung für die Informationssicherheit ist, die Wahrnehmung für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen sowie die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten zu vermitteln.

Ihre Vorteile:

- Erhöhung des Sicherheitsniveaus
- Sensibilisierung der Nutzer und Motivation für IT-Sicherheit
- Nachweise für Zertifizierungsanforderungen (z.B. ISO 27001)
- Kompakte Darstellung in max. 2 Stunden pro Nutzergruppe
- Individuelle Anpassung an Ihre vorhandenen Sicherheitsmaßnahmen

Vorgehensweise

VORBEREITUNG

- Abstimmung des Schulungsrahmens
- Abstimmung zu Regeln und Richtlinien der Kundenumgebung
- Anpassungswünsche durch den Kunden

MITARBEITERSCHULUNG

- Einführung in die Informationssicherheit
- Bedrohungslage mit Livedemos einfach und verständlich demonstriert
- Tipps und Tricks für den sicheren Umgang mit dem Internet

AUSWERTUNG

- Gemeinsame Auswertung der Schulungsmaßnahmen
- Definieren weiterer Schritte

SONDER-WORKSHOP
Windows-Hacking für Admins

In diesem ganztägigen Workshop erhalten Ihre Administratoren einen Überblick über gängige Angriffsvektoren in Active-Directory-verwalteten Netzwerken. Ziel ist, ein tiefergehendes Verständnis für Attacken zu vermitteln, um daraus ein eigenes Schutzkonzept entwickeln zu können. Gemäß dem Motto „Lernen durch Hacking“ führen wir Angriffe gemeinsam mit Ihren Admins durch, werten diese aus und zeigen Abwehrmaßnahmen. Hierbei werden Theorie und Praxis kompakt vermittelt.

Ihre Vorteile:

- Erste Analyse Ihrer Umgebung durch unsere erfahrenen Penetration-Tester
- Detailliertes Verständnis für gängige Angriffsvektoren im Windows-Umfeld
- Priorisierte Benennung von Härtungsmaßnahmen
- Sensibilisierung der Administratoren gegenüber Angriffen

„Regelmäßige Penetration Tests zeigen, dass in mittelständischen Unternehmen zu 90% keine Härtung des Microsoft Active Directory durchgeführt wird.

Im Workshop zeigen wir, wie Cyberkriminelle diese Lücke als Einfallstor in Ihre IT-Systeme nutzen.“

David Häntzschel
Cyber Security Consultant

LÖSUNG #2
Online-Schulung mit Phishing-Tests

Unsere Online-Schulungen stellen eine weitere Lösung zur Stärkung der Sicherheitskompetenz Ihrer Mitarbeitenden dar. Mit kurzen, animierten Lernvideos, realistischen Simulationen und gezielten Phishing-Tests unterstützen wir Sie dabei, Ihre Belegschaft effektiv zu schulen. Dank wissenschaftlich fundierter Methoden liefern wir Ihnen messbare Ergebnisse, die den Erfolg Ihrer Schulungsmaßnahmen belegen.

Ihre Vorteile:

- Jederzeit abrufbar & mehrsprachig
- Schulungen & Phishing-Tests aus einer Hand
- Individuell je nach Nutzerniveau angepasst
- Einfache Organisation, Einrichtung & Verwaltung
- Datenschutzkonforme Auswertungen

LÖSUNG #3
User Awareness as a Service

Nutzersensibilisierung sollte periodisch wiederholt werden, um nachhaltige Ergebnisse zu erzielen. Darum bieten wir auch „User Awareness as a Service“ an – ein kontinuierliches, automatisiertes und individuell anpassbares Schulungsprogramm. Durch regelmäßige Trainings, Simulationen und andere interaktive Methoden werden IT-Sicherheitsrisiken dauerhaft im Bewusstsein Ihrer Mitarbeitenden verankert. So erhöhen Sie langfristig die Cybersicherheit Ihres Unternehmens, indem Sie menschliche Fehler als Einfallstor für Angriffe reduzieren.

Enthaltene Leistungen:

1. **Konzeption** einer maßgeschneiderten Awareness-Strategie inklusive Ist-Analyse, KPI-Definition und Zeitplan-Erstellung
2. **Vor-Ort-Trainings** mit branchenspezifischen Übungen und Fallstudien sowie umfangreichem Schulungsmaterial für Teilnehmende

   Phishing-Tests mit simulierten Angriffen zur regelmäßigen Awareness-Überprüfung Ihrer Mitarbeitenden und gezielter Nachschulung

   Online-Trainings auf einer benutzerfreundlichen E-Learning-Plattform mit Quiz-Einheiten und Praxisbeispielen sowie automatisierter Erinnerung
3. **Mehrsprachigkeit** von Online-Trainings und Schulungsmaterial für globale Teams

   Rundum-Betreuung dank dediziertem Ansprechpartner, technischem Support und regelmäßigen Auswertungen

   Aktualität durch kontinuierliche Anpassung der Schulungsinhalte an neue Bedrohungslagen und Ihre Unternehmensbedürfnisse

Live Hacking, Admin Awareness und Phishing-Tests – mit unserer Expertise in offensiver und defensiver IT-Sicherheit machen wir Ihre Mitarbeiter fit gegen Cyberangriffe.

Sorgen Sie für mehr Sicherheit! Wir beraten Sie gern.

Ihr Security-Experte

Christian Müller · Principal Technology Consultant

Jetzt Beratungstermin vereinbaren:

kontakt@shd-online.de +49 (0)351 42 32 151

CISSP CCSP ECSA EC-Council Certified Security Analyst CHFI Computer Hacking Forensic Investigator

SHD. WIR BEWEGEN IT.

www.shd-online.de

ISO 9001 zertifiziert www.isocert.de TÜV SÜD ISO/IEC 27001

SHD System-Haus-Dresden GmbH
Zertifiziert nach ISO 9001 und ISO 27001

INDIVIDUELLE BERATUNG, PROJEKTARBEIT UND SERVICES RUND UM:

- IT-Infrastruktur & Cloud
- IT-Sicherheit
- Prozessmanagement

400-2.5-03.TFR