Layer 8
SECURITY AWARENESS

ALLGEIER
CyRis

IT-Sicherheitstraining, damit Ihre Mitarbeiter up-to-date sind und einen klaren Vorsprung haben

Layer8 – Security-Awareness-Training

Phishing-Versuche zu erkennen, ist Trainingssache, wie eine Sportübung. Liegt einer E-Mail, einer Website oder einem Anruf eine falsche Absicht zugrunde, gibt es immer auch entsprechende Hinweise darauf.

Mit Layer8, unserer Schulungsplattform für Security Awareness, lernen Ihre Mitarbeitenden, die Anzeichen von Phishing zu erkennen und korrekt zu reagieren. So werden sie in Sachen Informationssicherheit dauerhaft fit gemacht.

Vorgehen

Verschlüsselung der Mitarbeiterdaten

Während des Registrierungsprozesses wird ein zufälliger Schlüssel erstellt, mit dem alle Ihre Mitarbeiterdaten auf Layer8 verschlüsselt werden. Die von Ihnen gespeicherten Mitarbeiterdaten, dazu gehören Vor- und Nachname sowie die E-Mail-Adresse, werden mit Ihrem persönlichen Schlüssel durch AES-256-CBC gesichert.

Die Daten werden automatisch entschlüsselt und nach Verwendung bzw. nach Beendigung des HTTP-Requests wieder aus dem Arbeitsspeicher entfernt. Hochgeladene Dateien für den Import von Mitarbeiterdaten werden sofort nach der Verarbeitung gelöscht. Ihr eigenes Benutzerpasswort wird mit einem Salt-Wert versehen und durch Bcrypt gehasht in der Datenbank abgelegt.

Verarbeitung von sensiblen Daten

Im Rahmen von Phishing-Simulationen werden teilweise sensible Daten, wie Benutzername und Passwort von Mitarbeitern abgefragt, um verwertbare Ergebnisse für die Auswertungen zu erhalten. Um einen möglichen Missbrauch der Kundendaten entgegen zu wirken, wurden auf Layer8 folgende Sicherheitsfeatures integriert:

Bei allen Phishing-Szenarien wird eine Transportverschlüsselung über TLS erzwungen. Zusätzlich wird HTTP Strict Transport Security (HSTS) eingesetzt.

Die Verarbeitung der Zugangsdaten erfolgt nach einem Algorithmus, der sich für jeden einzelnen Empfänger und jede Kampagne ändert. Dieser ermöglicht die Aussage, ob unterschiedliche Benutzernamen- und Passwortkombinationen eingesetzt wurden.

Gleichzeitig verhindert der Algorithmus das Zurückführen der Hashwerte auf die ursprünglichen Zugangsdaten. Das Verfahren wurde mit großer Sorgfalt entworfen, um potenziellen Angreifern keine Angriffsfläche zu bieten.

E-Mail-Signaturen

Alle Schulungsinhalte, die über Layer8 gesendet werden, können mithilfe von S/MIME optional signiert werden. Dadurch können Ihre Mitarbeiter sicher sein, dass diese Nachrichten tatsächlich von Layer8 stammen und somit vertrauenswürdig sind.

Sicherheit der Infrastruktur

Wir lassen unsere Server und Datenbanken durch regelmäßige Pentests überprüfen. Hierbei wird vor allem Fokus auf die OWASP-Top-10 und die aktuellen Empfehlungen des BSI gelegt. Unsere Server und Anwendungen werden stets mit den aktuellsten Patches versorgt, um größtmögliche Sicherheit zu bieten. Alle Daten werden in Deutschland gespeichert.

Alle Verbindungen werden durch TLS abgesichert. Auch die interne Serverkommunikation erfolgt über verschlüsselte Verbindungen.

Schutz der Mitarbeiter

Phishing-Simulationen mithilfe von Layer8 dienen der Überprüfung der Unternehmenssicherheit und nicht der einzelnen Mitarbeiter. Deshalb werden Mitarbeiter des Unternehmens durch Anonymität geschützt. Zur Durchführung einer Phishing-Simulation ist es daher notwendig, mindestens fünf Empfänger einer Gruppe zuzuweisen. Der Versand an Gruppen, welche weniger Empfänger enthalten, wird technisch blockiert.

Weiterhin führt Layer8 keine Zuordnung zwischen einzelnen Mitarbeitern und Phishing-Simulationen. Der Durchführende erhält lediglich eine auf Gruppenebene zusammengefasste Statistik ohne personenbezogene Daten über die durchgeführte Simulation. Anders verläuft die Auswertung von Schulungskampagnen. Bei diesen Kampagnen werden die Mitarbeiter namentlich aufgeführt, um den Schulungsnachweis für das eingesetzte ISMS erbringen zu können. Einzelne Aktionen (Öffnen der E-Mail/Video angesehen/Quiz durchgeführt) werden hierbei als Nachweis in der Auswertung aufgeführt.

Die detaillierte Auswertung lässt sich selbstverständlich auch vom Layer8-Team deaktivieren, falls ihre Richtlinien dies nicht gestatten. Zudem können über das umfangreiche Rollensystem von Layer8 einzelnen Personen individuelle Rechte vergeben werden.

Schutz des Unternehmens

Selbstverständlich ist technisch sichergestellt, dass Unternehmen und Organisationen nur ihre eigenen Mitarbeiter durch Phishing-Simulationen überprüfen und Schulungsinhalte verteilen können. Dazu wird schon während der Erstellung des Accounts nur die Domain freigeschaltet, welche in der E-Mail-Adresse des Benutzers enthalten ist.

Außerdem sind die üblichen Maildienste und Domains gesperrt, da Layer8 nur für den Einsatz in Unternehmen und Organisationen bestimmt ist. Falls zusätzliche Domains zum Unternehmen gehören, können diese zur Freischaltung angewiesen werden. Wir überprüfen, ob die Domains zum Unternehmen gehören und schalten diese anschließend frei.

Impressum / V.i.S.d.P.

Herausgeber: Allgeier CyRis GmbH · Hans-Bredow-Straße 60 · 28307 Bremen

Redaktionsleitung: Sebastian Rüter · +49 40 389 071-172 · sebastian.rueter@allgeier-cyris.de

Grafikdesign: Tobias Wölky · www.woelky-grafik.de