OpenText Core Security Awareness Training

Risiken durch interne Benutzer reduzieren

Hauptvorteile

- 20 % weniger Malware im Vergleich zu Kunden mit OpenText Core Endpoint Protection
- Einfache Verwaltung und Kampagnenverwaltung
- Hohe Relevanz und Häufigkeit von Schulungsaktualisierungen mit nützlichen, interaktiven und effektiven Inhalten
- Integrierte Lösung für MSPs und KMUs mit Multi-Tenant-Management
- Automatisiertes Schulungsmanagement und Konformitätsberichte auf individueller, Gruppen- und Unternehmensebene

Phishing ist die beliebteste Methode von Hackern, da es einfach einzusetzen ist und 74 % dieser Phishing-Angriffe auf US-Unternehmen erfolgreich sind.[1] Unabhängig von der Größe eines Unternehmens ist es ein Ziel für Cyberkriminelle. Denn schon ein einziger unbedachter Klick auf einen Phishing-Link reicht aus, um Kriminellen Zugriff auf alle Daten in einem Netzwerk und in einigen Fällen sogar darüber hinaus zu gewähren. Aus diesem Grund sind Schulungen zum Sicherheitsbewusstsein und Phishing-Simulationen für Unternehmen unerlässlich, die Endnutzer vom schwächsten Glied in der Sicherheitskette zu einer wirklich widerstandsfähigen ersten Verteidigungslinie im Cyberbereich machen möchten.

Die beste Sicherheit der Welt kann nicht verhindern, dass ein Mitarbeiter, der vor Ort oder aus der Ferne arbeitet, versehentlich die Tür zum Netzwerk öffnet. OpenText Core Security Awareness Training unterstützt Unternehmen dabei, Endbenutzer zu befähigen, Betrugsversuche zu erkennen und zu melden, Risiken zu vermeiden, gesetzliche Vorschriften einzuhalten und moderne Cyberangriffe durch regelmäßige Schulungen im Rahmen eines mehrschichtigen Verteidigungsansatzes zu verhindern, um Cyberresilienz zu erreichen.

Risiken mit OpenText Core Security Awareness Training reduzieren

Mit neuen Bedrohungen und Angriffsvektoren Schritt halten

OpenText Core Security Awareness Training bietet kontinuierliche, relevante und messbare Schulungen und Tests, die Unternehmen benötigen, um riskante Benutzerverhalten zu minimieren und Cyberresilienz zu erreichen. Der Phishing-Simulator mit vollem Funktionsumfang bietet eine ständig wachsende Vorlagenbibliothek, die auf realen Szenarien basiert. Vorlagen werden kategorisiert und regionalisiert, um die Verwendung zu erleichtern, während die Zuordnung nach Zeitplänen eine gestaffelte Bereitstellung ermöglicht, um die Kampagnenwirkung zu maximieren.

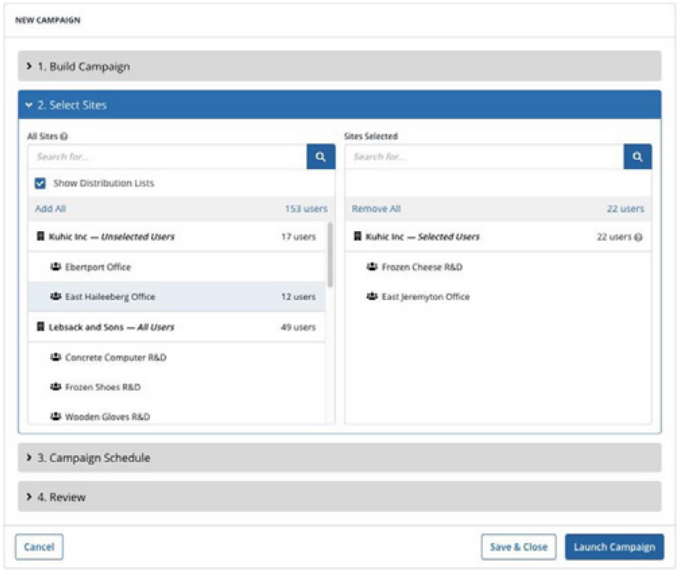
OpenText Core Security Awareness Training ist ein vollständig Cloud-basiertes Software-as-a-Service (SaaS)-Angebot. Administratoren können Schulungen und Phishing-Simulationen über die gleiche Konsole wie OpenText Core Endpoint Protection und OpenText Core DNS Protection verwalten. Das bedeutet, dass eine einheitliche Oberfläche mit geringen Gemeinkosten zur Verfügung steht. Gut geschulte Benutzer reduzieren die Anzahl der Sicherheitsvorfälle, mit denen ein Unternehmen konfrontiert wird, was wiederum die Kosten sowie die Verluste in Bezug auf Produktivität und Ausfallzeiten verringert. Nach unseren Beobachtungen bei Kunden aus der Praxis sind Unternehmen, die OpenText Core Security Awareness Training zusammen mit unserer Endpoint Security einsetzen, um 20 % weniger Malware ausgesetzt als Unternehmen, die nur unsere Endpoint Security einsetzen und keine Schulungen durchführen.

1 Venure Beat 2021: Phishing attacks get smarter as targets struggle to keep up

Mit der Option für eine Einzel- und Multi-Client-Konsole können Schulungen einfach an einem einzelnen Standort oder an mehreren Standorten durchgeführt werden

So funktioniert's

OpenText Core Security Awareness Training umfasst ein hochautomatisiertes Lernmanagementsystem (LMS), um das Schulungsmanagement einfach und effizient zu gestalten. Dank der Integration von Microsoft® Azure Active Directory können Administratoren mit OpenText Core Security Awareness Training den Import von Zielbenutzern automatisieren und diese synchron halten. Mit dem einfachen Einrichtungsassistenten können Sie ganz einfach Phishing-Simulationen und Schulungskampagnen erstellen. In wenigen Minuten können Sie eine Kampagne benennen, die gewünschten Empfänger auswählen, den Inhalt auswählen und starten. Administratoren können mehrere Schulungen und Phishing-Simulationen über einen bestimmten Zeitraum planen. Darüber hinaus können Administratoren, die mehrere Kunden oder Standorte verwalten, wie z. B. MSPs, diese Programme über mehrere Kunden hinweg auf globaler Ebene implementieren und verwalten. Funktionen für die Planung, zufällige Festlegung von Lieferzeiten, automatische Erinnerungen und Berichterstellung vereinfachen die Durchführung vollständig nachvollziehbarer und kontinuierlicher Kampagnen zur Sensibilisierung für Sicherheitsfragen, die das Benutzerverhalten im Laufe der Zeit effektiv verbessern.



OpenText Core Security Awareness Training

Die Azure AD-Integration vereinfacht die Verwaltung von Benutzerschulungen, während der Kampagnenassistent den Zeit- und Kostenaufwand für die Verwaltung von Schulungsprogrammen zur Cybersicherheit reduziert. Das integrierte LMS verfolgt die Teilnahme jedes Benutzers und macht alle Schulungen zur Cybersicherheit nachvollziehbar und messbar. In unserem zusammenfassenden Bericht zur Kampagne werden die Kampagnendaten und die Ergebnisse der Schulung hervorgehoben. Ein Schulungs-Dashboard mit einem einzigen Fenster zeigt alle laufenden oder abgeschlossenen Kampagnen an, während ein intuitiver Kampagnenmanagement-Workflow es Administratoren ermöglicht, Multi-Client-Schulungen schnell und einfach zu erstellen und zu starten.

OpenText Core Security Awareness Training ist ein schlüsselfertiges Programm zur Sensibilisierung für Sicherheitsfragen, bei dem Sie die Liste der Benutzer verwalten und wir diesen monatlich Schulungen und Phishing-Kampagnen zusenden.

Endnutzer vom schwächsten Glied in der Sicherheitskette in eine wirklich widerstandsfähige erste Verteidigungslinie im Cyberbereich verwandeln

Kontinuierliche, relevante und messbare Schulungen zur Minimierung riskanter Benutzerverhaltensweisen und zur Erreichung einer Cyberresilienz

OpenText Security Solutions vereint branchenführende Lösungen, die Ihr Unternehmen dabei unterstützen, cyberresilient zu bleiben. OpenText kann Ihnen dabei helfen, das Aufkommen von Bedrohungen bereits im Ansatz zu verhindern und die Folgen einer erfolgreichen Attacke durch eine schnelle Erkennung und eine nahtlose Wiederherstellung betroffener Daten möglichst gering zu halten, damit Sie die sich immer ändernden behördlichen Vorschriften weiterhin einhalten können.

Der umfangreiche Schulungskatalog von OpenText Core Security Awareness Training wird monatlich aktualisiert, um eine Vielzahl von sicherheits- und geschäftsbezogenen Themen in verschiedenen Formaten abzudecken. Sie können Phishing-Kampagnenstatistiken empfangen und Aktionen für einzelne Benutzer sowie andere Berichte erstellen, um Fortschritt und ROI zu messen. In einer kürzlich veröffentlichten Kundenübersicht über Phishing-Simulationen gaben 11 % der Benutzer an, auf die erste Phishing-E-Mail geklickt zu haben. Nach der sechsten Simulation war die Klickrate auf 6 % gesunken, nach der 18. Simulation auf 4 %. OpenText Core Security Awareness Training kann dazu beitragen, die Cyberresilienz bei Benutzern mit Themen zu erhöhen, die vom NIST Cybersecurity Framework empfohlen werden.

ELOVADE

Kontaktdaten für Deutschland & Österreich:
ELOVADE Deutschland GmbH
security@elovade.com
DE: +49 6441 67118 842
elovade.com/opentext-cybersecurity
AT: +43 820 0010 36

Kontaktdaten für die Schweiz:
ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/opentext-cybersecurity