Webroot®
Security Awareness Training

Reduzieren Sie das Risiko, das durch interne Benutzer entstehen kann

Übersicht

Phishing ist die beliebteste Wahl für Hacker, da es leicht eingesetzt werden kann und 74 % dieser Phishing-Angriffe auf US-Unternehmen erfolgreich sind.[1] Egal wie groß oder klein ein Unternehmen ist, es ist ein Ziel für Cyberkriminelle. Denn nur ein einziger unwissentlicher Klick auf einen Phishing-Link genügt, um Kriminellen Zugriff auf alles in einem bestimmten Netzwerk und in manchen Fällen sogar darüber hinaus zu gewähren. Das ist auch der Grund, warum Sicherheitsschulungen und Phishing-Simulationen für Unternehmen unerlässlich sind, die Endbenutzer vom schwächsten Glied in der Sicherheitskette zu einer wirklich widerstandsfähigen ersten Linie der Cyberverteidigung machen wollen.

Die beste Sicherheit der Welt kann nicht verhindern, dass ein unwissender Mitarbeiter, der vor Ort oder aus der Ferne arbeitet, versehentlich die Tür zum Netzwerk weit offen lässt. Webroot® Security Awareness Training unterstützt Unternehmen dabei, Endbenutzer in die Lage zu versetzen, Betrug zu erkennen und zu melden, Risiken zu vermeiden, gesetzliche Vorschriften einzuhalten und moderne Cyberangriffe durch regelmäßige Schulungen als Teil eines mehrschichtigen Verteidigungsansatzes zu verhindern.

Risikominimierung durch Schulungen zum Sicherheitsbewusstsein

Bleiben Sie auf dem Laufenden über sich entwickelnde Bedrohungen und neue Angriffsvektoren

Webroot® Security Awareness Training bietet kontinuierliche, relevante und messbare Schulungen und Tests, die Unternehmen benötigen, um riskantes Benutzerverhalten zu minimieren und Cyber-Resilienz zu erreichen. Der voll funktionsfähige Phishing-Simulator bietet eine ständig wachsende Vorlagenbibliothek, die auf realen Szenarien basiert. Die Vorlagen sind kategorisiert und regionalisiert, um die Verwendung zu erleichtern, während die Randomisierung des Zeitplans eine gestaffelte Auslieferung ermöglicht, um die Wirkung der Kampagne zu maximieren.

Webroot® Security Awareness Training ist ein vollständig cloudbasiertes Software-as-a-Service (SaaS) Angebot. Administratoren können Schulungs- und Phishing-Simulationen über dieselbe Konsole wie Webroot® Business Endpoint Protection und Webroot® DNS Protection verwalten und so eine Single-Pane-of-Glass-Erfahrung mit geringem Verwaltungsaufwand bieten. Gut geschulte Benutzer reduzieren die Anzahl der Sicherheitsvorfälle, mit denen ein Unternehmen konfrontiert wird, was wiederum die Kosten sowie Produktivitätsverluste und Ausfallzeiten reduziert. Unseren Beobachtungen von Kunden aus der Praxis zufolge sind Unternehmen, die Webroot® Security Awareness Training zusammen mit unserer Endpunktsicherheit einsetzen, mit 20 % weniger Malware konfrontiert als Unternehmen, die nur unseren Endpunktschutz einsetzen und kein Training absolvieren.

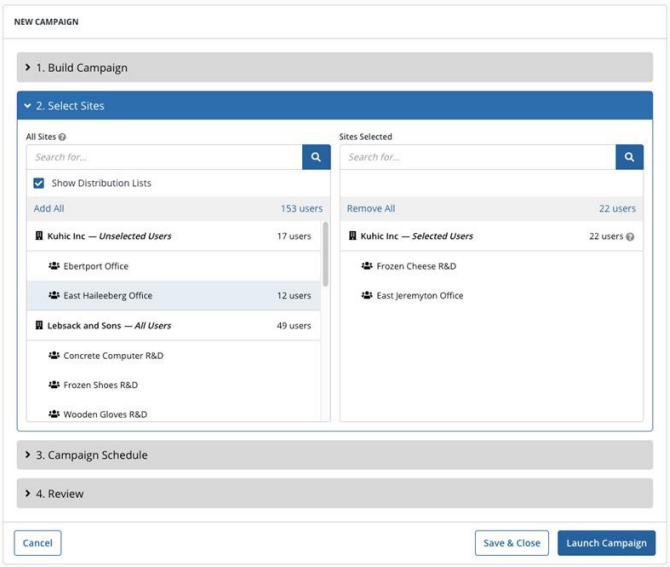
Wichtigste Vorteile

- 20 % weniger Malware im Vergleich zu Kunden, die ausschliesslich Webroot Endpoint Protection allein benutzen
- Einfache Verwaltung und Kampagnenmanagement
- Hohe Relevanz und Häufigkeit der Schulungsaktualisierungen mit nützlichen, interaktiven und der Realität angepassten Inhalten
- Integrierte Lösung für MSPs und KMUs mit mandantenfähiger Verwaltung
- Automatisiertes Trainings-management und Compliance-Berichte auf Einzel-, Gruppen- und Unternehmensebene

Einzel- und Mehrmandanten-Konsolen-option, mit der Sie Schulungen problemlos an einem oder mehreren Standorten durchführen können

Wie es funktioniert

Webroot® Security Awareness Training umfasst ein hoch automatisiertes Learning Management System (LMS), das die Verwaltung von Schulungen einfach und effizient macht. Mit der Microsoft® Azure Active Directory-Integration können Administratoren mit Webroot® Security Awareness Training den Import von Zielbenutzern automatisieren und diese auf dem gleichen Stand halten. Der einfache Einrichtungsassistent erleichtert das Erstellen von Phishing-Simulationen und Trainingskampagnen. In nur wenigen Minuten können Sie eine Kampagne benennen, die gewünschten Empfänger auswählen, den Inhalt auswählen und starten. Administratoren können eine Abfolge von mehreren Schulungen und Phishing-Simulationen über einen bestimmten Zeitraum planen. Darüber hinaus können Administratoren, die mehrere Kunden oder Standorte verwalten, wie z. B. MSP, diese Programme für mehrere Kunden auf globaler Ebene implementieren und verwalten. Funktionen für die Zeitplanung, die Randomisierung der Auslieferungszeit, automatische Erinnerungen und Berichte machen es einfach und unkompliziert, vollständig rechenschaftspflichtige und kontinuierliche Sicherheitskampagnen durchzuführen, die das Benutzerverhalten im Laufe der Zeit effektiv verbessern.



Webroot Security Awareness Training-Konsole

Die Azure AD-Integration macht die Verwaltung von Benutzerschulungen einfach, während der Kampagnen-Assistent den Zeit- und Kostenaufwand für die Verwaltung von Cybersecurity-Schulungsprogrammen reduziert. Das integrierte LMS verfolgt die Teilnahme jedes Benutzers und macht die gesamte Cybersicherheitsschulung nachvollziehbar und messbar. Unser zusammenfassender Bericht zur Kampagne zeigt die Daten der Kampagne und die Ergebnisse der Schulung auf. Ein übersichtliches Trainings-Dashboard zeigt alle laufenden oder abgeschlossenen Kampagnen an, während ein intuitiver Kampagnenmanagement-Workflow es Administratoren ermöglicht, schnell und einfach Multi-Client-Trainings zusammenzustellen und zu starten.

Webroot SAT enthält jetzt Autopilot, ein schlüsselfertiges Programm zur Erhöhung des Sicherheitsbewusstseins, bei dem Sie die Liste der Benutzer verwalten; wir senden ihnen monatlich Schulungen und Phishing-Kampagnen.

Ermöglichen Sie dem Endbenutzer vom schwächsten Glied in der Sicherheitskette vollständig widerstandsfähig gegenüber den Cyberangriffen zu werden

Kontinuierliche, relevante und messbare Aufklärung, um riskantes Nutzerverhalten zu minimieren und Cyber-Resilienz zu erreichen

OpenText Security Solutions vereint erstklassige Lösungen, die Ihrem Unternehmen helfen, cyber-resilient zu bleiben. Carbonite und Webroot können Sie dabei unterstützen, Bedrohungen von vornherein zu verhindern und zu schützen, die Auswirkungen durch schnelle Erkennung und Reaktion zu minimieren, die Daten nahtlos wiederherzustellen, um die Auswirkungen zu verringern, und Sie bei der Anpassung und Einhaltung der sich ändernden Vorschriften zu unterstützen.

Der umfangreiche Schulungskatalog von Webroot® Security Awareness Training wird monatlich aktualisiert und deckt eine Vielzahl von sicherheits- und geschäftsbezogenen Themen in verschiedenen Formaten ab. Sie können Statistiken über Phishing-Kampagnen erhalten und Berichte über Aktionen pro Benutzer und andere Berichte erstellen, um den Fortschritt und den ROI zu messen. Bei einer kürzlich durchgeführten Kundenbefragung zu Phishing-Simulationen klickten 11 % der Benutzer auf die erste Phishing-E-Mail. Bei der 6. Simulation war die Klickrate auf 6 % gesunken, bei der 18. Simulation lag sie bei 4 %. Webroot® Security Awareness Training kann dazu beitragen, die Cyber-Resilienz der Benutzer mit den vom NIST Cybersecurity Framework empfohlenen Themen zu stärken.

[1] Venure Beat 2021, Phishing attacks get smarter as targets struggle to keep up

Über Carbonite und Webroot

Carbonite und Webroot, Unternehmen von OpenText, nutzen die Cloud und künstliche Intelligenz, um umfassende Cyber-Resilienz-Lösungen für Unternehmen, Privatpersonen und Managed Service Provider anzubieten. Cyber-Resilienz bedeutet, dass Sie in der Lage sind, selbst bei Cyberangriffen und Datenverlusten den Betrieb aufrechtzuerhalten. Deshalb haben wir unsere Kräfte gebündelt, um Lösungen für den Schutz von Endpunkten, den Schutz von Netzwerken, die Schulung des Sicherheitsbewusstseins, die Datensicherung und die Notfallwiederherstellung sowie Bedrohungsanalysen anzubieten, die von marktführenden Technologieanbietern weltweit genutzt werden. Wir nutzen die Möglichkeiten des maschinellen Lernens, um Millionen von Unternehmen und Privatpersonen zu schützen und die vernetzte Welt zu sichern. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Erfahren Sie mehr über Cyber-Resilienz unter carbonite.com und webroot.com.

Erfahren Sie mehr unter webroot.com

CARBONITE® + WEBROOT®
OpenText-Sicherheitslösungen