Perseus 360° Cybersicherheit

Leistungsbeschreibung

Im Folgenden finden Sie unsere Leistungen im Überblick:

1. Führerschein für Datenschutz
Mit Hilfe des Video-Trainings lernen Kunden in acht Lektionen die Grundlagen des Datenschutzes kennen. Das Thema wird mit einfachen Worten dargestellt und anhand von praktischen Beispielen erklärt. Auf jede Video-Lektion folgt ein kurzer Test. Wurden alle Lektionen erfolgreich absolviert, erhalten Mitarbeiter ein Zertifikat – den Führerschein für Datenschutz.

2. Führerschein für Cybersicherheit
Mit dem Führerschein für Cybersicherheit lernen Kunden in acht Lektionen, wie Sie sich vor Cyberangriffen schnell und effektiv schützen können. Jede Lektion besteht aus einem Trainingsvideo und einem anschließenden Test. Wurden alle Lektionen erfolgreich absolviert, erhalten Mitarbeiter ein Zertifikat – den Führerschein für Cybersicherheit.

3. Cockpit für den Administrator
Der Administrator erhält eine Mitarbeiterübersicht in Form eines Cockpits mit Schulungsstatistiken zum Cyber- bzw. Datenschutz-Führerschein, downloadbar als CSV/Excel-Datei. Dazu werden Sicherheitsstatistiken zu z.B. zu Phishing-Tests aufgeführt.

4. Phishing-Tests
Mit fingierten Betrugs-E-Mails wird das Gefahrenbewusstsein der Mitarbeiter überprüft, inklusive Reportingmöglichkeit. Perseus führt regelmäßig Phishing-Tests mit verschiedenen Phishing-Vorlagen durch. Tracking-Links sind in diesen Vorlagen eingebettet, so dass das Nutzerverhalten überprüft werden kann. Wenn der Nutzer fälschlicherweise auf Anhänge oder Links in der Betrugs-E-Mail klickt, wird er auf eine Webseite geleitet, die ihm erklärt, was Phishing ist. Außerdem werden dort Links zu weiteren Materialien (Kursthema/Blogartikel über Phishing) bereitgestellt. Die Ergebnisse von Phishing-Tests sind für den Administrator im Administrator-Cockpit auf der Plattform sichtbar.

5. E-Mail-Scanner
Im Zweifel “Safety first”. Der Nutzer kann Perseus eine verdächtige E-Mail zukommen lassen. Alle Anhänge werden auf bekannte Malware-Signaturen überprüft, alle Links werden mit einer sicheren Datenbank, in der verdächtige Webseiten gesammelt werden, abgeglichen. Das Ergebnis erhält der Kunde von Perseus per E-Mail, sobald der Scan abgeschlossen ist (<15 min).

6. Browser-Check
Browser regelmäßig auf Updates überprüfen. Der Kunde kann überprüfen, ob sein Browser auf dem neuesten Stand ist. Sollte dies nicht der Fall sein, erhält der User einen Link zu einem vertrauenswürdigen Anbieter, bei dem er seinen Browser auf die neueste Version aktualisieren kann.

7. Datensicherheits-Check – automatisiertes, konstantes Scannen von Mitarbeiter E-Mail-Adressen
Perseus prüft, ob in Verbindung mit der E-Mail-Adresse des Benutzers Sicherheitsvorfälle bekannt wurden, in dem die Adresse mit einer Datenbank zu aktuellen Sicherheitsvorfällen abgeglichen wird. Diese sammelt betroffene Nutzerdaten (z.B. Anmeldedaten, Passwörter, etc.) aus verschiedenen Quellen. Wir zeigen, auf welchen Webseiten der Benutzer kompromittiert wurde und empfehlen ihm, das Passwort zu ändern, wenn eines seiner Online-Konten im Dark Web "geleaked" wurde.

8. Passwort-Generator
Mit unserem Dienst helfen wir dem Kunden, sichere Passwörter zu generieren. Der Nutzer wählt einen Satz, an den er sich gut erinnern kann. Dieser muss 8 Elemente inklusive Klein- und Großbuchstaben sowie mindestens eine Zahl und ein Sonderzeichen (! @ # $% ^) enthalten. Jedes Wort, jede Zahl und jedes Zeichen müssen durch ein Leerzeichen getrennt sein. Aus den Anfangsbuchstaben wird schließlich ein persönliches Passwort gebildet. Zum Beispiel: "Ich gehe ab Juni mit 2 Freunden ins Fitnessstudio!" Das Passwort lautet: IgaJm2FiF!

9. Passwort-Erinnerung
Jeder Nutzer kann eine Erinnerung einrichten, die ihm alle 8 Wochen eine E-Mail mit einer Erinnerung sendet, um sein Passwort zu ändern. Außerdem werden dem Nutzer die Grundregeln für die Wahl eines neuen Passworts erklärt.

10. Expertengespräche
Unsere Experten stellen einzelne, relevante Themen für die Bereiche Cybersicherheit und Datenschutz in kurzen Beiträgen persönlich vor. Der Kunde profitiert von einer weiteren Informationsquelle, um sich gegen Cybergefahren zu schützen.

11. Kundenservice
Bei uns steht der Kunde im Mittelpunkt. Er soll den Perseus Service und dessen Vorteile optimal nutzen können. Daher kümmert sich unser Team aus erfahrenen Kundenbetreuern um alle Fragen von der ersten Nutzung des Kundenbereichs bis zur Klärung der Fragen rund um das Thema Cybersicherheit. Während unserer Geschäftszeiten steht der Service zur Verfügung.

12. Live-Chat
Kunden erwarten Service in Echtzeit. Aus diesem Grund bieten wir einen Live-Chat als Kommunikationskanal auf unserer Webseite und im Mitgliederbereich an. Während unserer Geschäftszeiten steht der Service zur Verfügung.

13. Checkliste
Damit Kunden für die Themen Cybersicherheit und Datenschutz gewappnet sind, haben wir eine Checkliste mit einigen Anregungen für mögliche organisatorische und technische Maßnahmen in Unternehmen zusammengestellt.

14. Newsletter & Blog-Artikel
Kunden werden über aktuelle gesellschaftliche, rechtliche und technische Entwicklungen im Bereich der Cybersicherheit informiert.

15. Angriffsalarm
Perseus warnt die Kunden vor aktuellen Angriffswellen durch Viren, Trojaner oder Phishing per E-Mail.

16. Endpoint-Detection & Response (EDR)
Schützt wie ein Antivirenscanner, nur dass durch maschinelles Lernen und künstliche Intelligenz auch Abwandlungen von bekannter Schadsoftware erkannt werden. Bei Unregelmäßigkeiten werden die Endgeräte zusätzlich von Sicherheitsexperten geprüft. Die intelligente Sicherheitssoftware wird in Kooperation mit der Firma Cylance by Blackberry angeboten. Das Produkt besteht aus zwei Komponenten: Cylance Protect – zum Schutz vor Schadsoftware, Cylance Optics – zum Monitoring durch unsere Experten.

17. IT-Sicherheitsprüfung mit Score
Wir erstellen einen Sicherheitsbericht basierend auf einem Scan der öffentlich erreichbaren Infrastruktur des Kunden. Das Unternehmen wird in den Bereichen Server- und Netzwerksicherheit, IT-Sicherheitskultur und Prozesse und Sicherheit von Endgeräten überprüft. Zusätzlich müssen 9 Fragen beantwortet werden, um den Sicherheitsbericht erstellen zu können. Kunden erhalten ihren individuellen Sicherheitsbericht mit Score als PDF während der Geschäftszeiten innerhalb von 24 Stunden.

18. Notfallhilfe (FNOL)
Unsere Experten von der Hotline für Cybersicherheit helfen Mitgliedern, bei einer Cyberattacke wieder zurück ins Geschäftsleben zu kommen. Das Unternehmen erhält folgende Vorteile: Analyse des Vorfalls, Bewertung des Schadensausmaßes, konkrete Handlungsempfehlungen, Hilfe bei Datenwiederherstellung, Dokumentation und Nachsorge. Dieser Service steht 24/7 zur Verfügung.

19. Partnernetzwerk
Bei größeren Schadensfällen, die sich nicht telefonisch innerhalb von vier Stunden beheben lassen, empfehlen wir spezialisierte Partner wie IT-Experten, Rechtsanwaltskanzleien oder PR-Agenturen.

20. Perseus Schutzbrief für die Kostenübernahme bei Cybervorfällen

Der Schutzbrief übernimmt die Kosten, die von Perseus und seinen Partnern zur Wiederherstellung der IT-Systeme erbracht werden, die aber nicht im Standard des Premium Angebotes enthalten sind. Die Schutzbrief stellt sicher, dass alle notwendigen Maßnahmen zur schnellen Wiederaufnahme des ordnungsgemäßen Geschäftsbetriebs sofort eingeleitet werden können. Dafür übernimmt er die externen Kosten bis zu 50.000 € pro Jahr für:

1. den Einsatz von IT-Forensik-Experten vor Ort
2. für die Systemwiederherstellung und die Entfernung der Schadsoftware
3. für die Systemverbesserung und Prävention nach Angriff
4. für die Dokumentation und Rechtsberatung im Rahmen der DSGVO und für die Einhaltung der Meldepflichten

Die genauen Leistungen entnehmen Sie bitte der Leistungsbeschreibung des Schutzbriefes.