redIT

«REDIT SECURITY TRAININGS»

LEISTUNGSBESCHREIBUNG / NUTZUNGSBEDINGUNG

Inhaltsverzeichnis

1 EINLEITUNG

Die Security Produkte wurden von unseren Security-Spezialisten entwickelt, um KMU im Bereich der IT-Sicherheit auf einen aktuellen und sicheren Stand zu bringen. Es wendet sich an alle IT-sicherheitsbewusste Unternehmen, welche den Risikofaktor Mitarbeiter durch eine durch Spezialisten durchgeführte Schulung minimieren möchten oder die Security Awareness ihrer Mitarbeiter direkt schulen möchten.

2 Service Levels

- 7 X 24h Störungsannahme (E-Mail und *Telefon)
  (*nur für Kunden mit separaten Wartungsverträgen! Ansonsten gilt Mo - Fr 07.00 17.00)

3 Security Awareness Training

3.1 Produktspezifikationen

3.1.1 Zweistündige Schulung zu den untenstehenden Themen

- Aktuelle Gefahren
- E-Mail Security
- Phishing
- SPAM
- Ransomware
- Schadsoftware
- Betrügerischer Verkauf
- Aufbau des Internets
- Deep Web / Dark Web
- Passwortsicherheit
- Social Engineering

3.1.2 Prüfung mit Zertifikat

Einheitliche Prüfung nach der Schulung, in welcher sich die anwesenden Mitarbeiter das «redIT-Security» Zertifikat verdienen können.

- Die Prüfung erfolgt in elektronischer Form mit einem von redIT bereitgestellten Tool
- Dem Kursteilnehmer wird ein Zertifikat nach Erfolg zugestellt

3.2 Voraussetzungen

Das Unternehmen, welches die Schulung in seinen eigenen Räumlichkeiten wünscht, muss folgende Punkte zur Verfügung stellen:

- Anwesenheit des IT-Verantwortlichen
- Sitzungszimmer / Konferenzraum mit genügend Sitzplätzen für angemeldete Nutzer
- Internet- / Mobilfunkanschluss
- HDMI-fähiger Beamer oder Grossraum Screen

4 Phishing Simulation

Eine Phishing Kampagne ermöglicht Ihnen Ihre Mitarbeiter gegen mögliche Phishing Angriffe zu sensibilisieren. Zusätzlich erhalten Sie Daten und Einblicke zum Verhalten Ihrer Mitarbeiter beim Erhalt der Phishing-E-Mail.

4.1 Produktspezifikationen

Die Phishing Kampagne wird mit dem Angriffssimulationstraining von Microsoft durchgeführt. Es können maximal 4 Phishing Kampagnen pro Monat gebucht werden. Die technische Einrichtung wird dabei durch die redIT übernommen. Die professionelle Gestaltung der Phishing E-Mails wird ebenfalls durch die redIT durchgeführt. Nach der Phishing Kampagne wird eine Auswertung durchgeführt und an die zuständige Ansprechperson zugestellt.

4.1.1 Voraussetzungen

- Der Kunde muss über einen M365 Tenant verfügen
- Die Benutzer, welche an der Phishing Kampagne teilnehmen, müssen ein Exchange Online Postfach haben.
- redIT muss zwecks Einrichtung und Erstellung der Phishing Kampagne Zugang zum Administratoren Portal von Microsoft gewährt werden.
- Mitarbeiter müssen in einem Excel mit Vor- und Nachnamen sowie E-Mail-Adresse geliefert werden

4.1.2 Lizenzen

Pro Mitarbeitenden und Monat wird eine Defender for Office 365 Plan 2 (Add On) Lizenz benötigt.

5 Sophos Phish Threat

Sophos Phish Threat liefert Ihnen flexible, individuell anpassbare Mail-Vorlagen, welche Sie auf Ihre Mitarbeiter zuschneiden können, um die Phishing-Awareness Ihrer Mitarbeiter zu testen. Sophos Phish Threat liefert Ihnen zusätzlich Daten zum Verhalten Ihrer Mitarbeiter beim Erhalt dieser E-Mails. Der Kunde erhält bei Kauf des Produktes Zugang zum Portal für das selbständige Testen der Mitarbeiter.

5.1 Produktspezifikationen

5.1.1 Lizenzen

Pro Mitarbeitenden und Monat, wird eine Lizenz benötigt.

5.2 Verrechnung

Der Stichtag für die Abrechnung einer Periode ist der 22. des Monates, wenn der 22. auf ein Wochenende oder einen Feiertag fällt, wird der Werktag zuvor genommen. Wird das Produkt nach dem 22. eines Monats verwendet wird diese Periode ebenfalls abgerechnet.

6 Kombipaket Security Awareness Training & Phishing Simulation

Kombination der beiden Produkte Security Awareness Training und Phishing Simulation.

6.1 Produktspezifikationen

6.1.1 Zweistündige Schulung zu den untenstehenden Themen

- Aktuelle Gefahren
- E-Mail Security
- Phishing
- SPAM
- Ransomware
- Schadsoftware
- Betrügerischer Verkauf
- Aufbau des Internets
- Deep Web / Dark Web
- Passwortsicherheit
- Social Engineering

6.1.2 Prüfung mit Zertifikat

Einheitliche Prüfung nach der Schulung, in welcher sich die anwesenden Mitarbeiter das «redIT-Security» Zertifikat verdienen können.

- Die Prüfung erfolgt in elektronischer Form mit einem von redIT bereitgestellten Tool
- Dem Kursteilnehmer wird ein Zertifikat nach Erfolg zugestellt

6.1.3 Phishing Simulation

- 2 Phishing-Kampagnen pro Monat über eine Zeitdauer von 3 Monaten
- 2 Phishing-Kampagnen vor dem Security Awareness Training, 4 danach
- Recherche mithilfe Unternehmung um die Attacke so authentisch wie möglich zu fahren
- Analyse des Nutzerverhaltens beim Erhalt von Phishing-Mails
- Grafische Darstellung der Daten

6.2 Voraussetzungen

Das Unternehmen, welches die Schulung in seinen eigenen Räumlichkeiten wünscht, muss folgende Punkte zur Verfügung stellen:

- Anwesenheit des IT-Verantwortlichen
- Sitzungszimmer / Konferenzraum mit genügend Sitzplätzen für angemeldete Nutzer
- Internet- / Mobilfunkanschluss
- HDMI-fähiger Beamer oder Grossraum Screen

Des Weiteren sind folgende Punkte erforderlich:

- Der Kunde muss über einen M365 Tenant verfügen
- Die Benutzer, welche an der Phishing Kampagne teilnehmen, müssen ein Exchange Online Postfach haben.
- redIT muss zwecks Einrichtung und Erstellung der Phishing Kampagne Zugang zum Administratoren Portal gewährt werden.
- Mitarbeiter müssen in einem Excel mit Vor- und Nachnamen sowie E-Mail-Adresse geliefert werden

7 NICHT ENTHALTENE LEISTUNGEN

- Fahrtweg zum Kunden ausserhalb eines Radius von 30km ab einem redIT Standort nach Absprache.

8 ALLGEMEINE PRODUKTBESTIMMUNGEN

- Das Security Awareness Training ist in folgenden Regionen durchführbar: Deutschschweiz
- Die Schulung im Rahmen des Security Awareness Trainings findet in Schweizerdeutsch oder Hochdeutsch statt (Prüfung und Kursunterlagen ebenfalls in Deutsch)
- Die Kampagnen werden in Deutsch oder Englisch versandt
- redIT behält sich vor, Aufträge abzulehnen
- Es gelten unsere Allgemeinen Geschäftsbestimmungen

9 ALLGEMEINE BESTIMMUNGEN

redIT kann nicht für Konfigurations- oder Manipulationsfehler des Kunden oder Dritten haftbar gemacht werden. Für Services, bei welchen Systemressourcen geteilt verwendet werden (Shared Services), nimmt der Kunde Rücksicht und schränkt die übermässige Nutzung dieser Ressourcen ein, um eine Beeinträchtigung der Leistung anderer Kunden auf demselben System zu verhindern («Fair use»). Beansprucht der Kunde die Systemressourcen über Gebühr (Vergleich mit dem Durchschnitt der Systemnutzer plus Toleranz), unterbreitet redIT dem Kunden ein Angebot für eine höhere Leistungsklasse. Nimmt der Kunde dieses Angebot nicht an, behält sich redIT vor, fristlos vom Vertrag zurückzutreten.
Die Services werden «Best effort» gewährleistet. Es gibt, wo nicht anders vermerkt, keine Garantie für bestimmte zugewiesene Systemressourcen oder Leistungsmerkmale. Bestehen Anzeichen eines rechts- oder vertragswidrigen Verhaltens, insbesondere einer missbräuchlichen Nutzung eines Service, kann redIT den Zugriff auf den Service ohne Vorankündigung umgehend entschädigungslos sperren oder einschränken, den Kunden zur rechts- und vertragskonformen Benutzung anhalten, den Vertrag frist- und entschädigungslos auflösen und gegebenenfalls Schadenersatz sowie die Freistellung von Ansprüchen Dritter verlangen.
Sollten einzelne Bestimmungen dieser Leistungsbeschreibung/Nutzungsbedingung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen des jeweiligen Vertrags nicht tangiert.