Leistungsbeschreibung

Security Awareness Service (SAS)

Der Security Awareness Service bietet ein kontinuierliches **Security Training für Mitarbeiter** (im Folgenden Benutzer). Dabei werden zur Trainingssteuerung verschiedene Mechanismen in Form der Awareness Engine und der Spear-Phishing-Engine eingesetzt. Auf diese Weise **werden Mitarbeiter bedarfsgerecht trainiert**, um **Cyber-Angriffe sicher zu erkennen** und effektiv abzuwehren – ohne, dass sich Administratoren oder CISOs (im Folgenden Administrator) selbst in die zugrundeliegende Psychologie und Didaktik einarbeiten müssen.

Die Grundlage des Awareness Services bildet ein **patentiertes Verfahren zur Messung des Sicherheitsverhaltens** aller am Security Awareness Service teilnehmenden Gruppen und Benutzer. Auf Basis des gemessenen Sicherheitsverhaltens wird die wissenschaftliche Kennzahl **Employee Security Index (ESI®)** berechnet.

1. Der Security Awareness Service bietet den Benutzern die folgenden Funktionen:
   a. Administratoren können Benutzer im Control Panel über LDAP-Synchronisierung, über Microsoft 365-Synchronisierung oder über .csv-Upload erstellen, löschen und **kontinuierlich synchronisieren**.
   b. Die Awareness Engine bildet den technologischen Kern für den Security Awareness Service im Auto Pilot-Betriebsmodus. Sie wertet regelmäßig das Security-Verhalten der Benutzer aus und entscheidet auf dieser Grundlage, welche Benutzer zusätzliches Training oder Simulationen erhalten. Jeder Benutzer erhält je nach seinem Security-Level **den erforderlichen Umfang** an Training. Die Konfiguration umfasst eine **Single User Booster-Option** für Benutzer, die eine intensivere Schulung benötigen, und eine **Productivity Booster-Option** für starke Benutzer, die sich mehr auf ihre tägliche Arbeit konzentrieren können. Zu den Schulungsaktivitäten gehören **Spear-Phishing-Simulationen** und **E-Training-Inhalte**.

      Es ist möglich, die Trainingsmodule selbst zu orchestrieren und zu versenden, anstatt die Awareness Engine zu verwenden. Es können maximal 2 Trainingsmodule pro Monat versendet werden, um eine Überlastung der Benutzer zu vermeiden. In diesem Fall wird die Awareness Engine deaktiviert.

      Die patentierte Spear-Phishing-Engine erlaubt das Versenden von Spear-Phishing-E-Mails in verschiedenen Schwierigkeits-Leveln.
   c. Spear-Phishing-Simulationen sind besonders effektiv, um das Sicherheitsverhalten von Benutzern zu verändern:
      i. Erstens kann durch die Erzeugung eines **Effekts der „Selbsterfahrung"** das Mindset überwunden werden: „Mich greift doch sowieso keiner an".

ii. Zweitens bieten Phishing-Simulationen die Möglichkeit, kurze, relevante Lerninhalte in Form eines Nano-Learnings zu vermitteln: Auf der **Erklärseite** wird der Benutzer interaktiv aufgeklärt, wie er hätte erkennen können, dass diese E-Mail gefälscht war.

iii. Drittens ermöglicht eine Spear-Phishing-Simulation auf Basis der Spear-Phishing-Engine die Messung des aktuellen Employee Security Index (ESI®).

iv. Standardmäßig werden ca. zwei Spear-Phishing-E-Mails pro Monat je Benutzer versendet. Dabei erhält jeder Benutzer zu einem anderen Zeitpunkt eine andere E-Mail. Der Inhalt der E-Mail richtet sich nach Level (siehe v.), sowie vorhanden Informationen zum Unternehmen bzw. zum Benutzer selbst. Die **Intensität** kann per Konfiguration im Control Panel erhöht (drei E-Mails pro Monat) bzw. gesenkt (eine E-Mail pro Monat) werden.

v. Die **Level der Spear-Phishing-E-Mails** basieren auf standardisierten Einteilungen: je höher das Level, desto höher der Zeitaufwand eines Angreifers. Die automatische Auswahl von Spear-Phishing-E-Mails basiert auf verschiedenen Faktoren, wie z. B. Informationen über den einzelnen Benutzer, das Unternehmen, die Branche usw. Genau wie echte Angreifer verwenden sie ein vielfältiges Arsenal an Werkzeugen wie z. B. gefährliche Links, gefälschte Anmeldeseiten, Makros, Dateianhänge usw. Spear-Phishing-E-Mails werden in verschiedenen Schwierigkeitsgraden versandt, bei denen unter anderem **hochqualitatives Spear-Phishing** mit der Simulation von gefälschtem, internen E-Mail-Verkehr realisiert wird:

   Level 1: Massen-Phishing

   Level 2: gezieltes Phishing sogenannter CEO-Frauds

   Level 3: Spear-Phishing unter Einbeziehung von Informationen über das Unternehmen

   Level 4: Spear-Phishing mit Bezug zur individuellen Job-Position des Empfängers sowie E-Mails von direkten Kollegen oder Vorgesetzten.

   Level 5: Spear-Phishing mit Domain-Spoofing

vi. Ein Benutzer muss zunächst ein Level „bestehen", bevor er sich in das nächste Level steigern kann. Sollte er auf eine Spear-Phishing-E-Mail hereinfallen, wird er um ein Level zurückgestuft. So wird sichergestellt, dass Benutzer nicht überfordert, sondern jeweils auf ihrem **individuellen Sicherheitsniveau abgeholt** werden und dieses sukzessive gesteigert wird.

vii. Beim **Credential-Phishing** wird mittels fingierter Anmeldeseiten geprüft, wie viele Benutzer ihre Zugangsdaten auf einer gefälschten Webseite eingeben. Während der Phishing-Simulation werden dabei unter keinen Umständen Login-Daten an unsere Server übermittelt oder gespeichert.

viii. Beim **Malware-Phishing** wird mittels fingierter Dateianhänge geprüft, wie viele Benutzer einen Office-Anhang öffnen und ein Makro aktivieren. Die verwendeten Dateianhänge können beispielsweise .docm- und .xlsm-Dateien enthalten. Sie werden jedoch nach Bedarf auf ihre Relevanz geprüft und ggf. verändert. Beim Öffnen einer Datei oder aktivieren von einem Makro wird unter keinen Umständen Malware ausgeführt.

d. **Erklärseite: Most Teachable Moment** – Hornetsecurity liefert relevante Lerninhalte, wenn die Lernbereitschaft am größten ist – nämlich in dem Moment, wenn der Benutzer auf eine Phishing-Mail hereingefallen ist. Auf der interaktiven Erklärseite mit **individuellen**

Trainingsinhalten zu der gerade simulierten E-Mail wird in einem Nano-Learning vermittelt, wie ein echter Angriff hätte erkannt und abgewehrt werden können. Dabei werden sowohl eindeutige Erkennungszeichen sowie psychologische Tricks der Angreifer aufgezeigt.

e. Der **Phishing Reporter** ist ein **Outlook-Add-In für Desktop und mobile Endgeräte**. Er vereinfacht den Meldeprozess für reale Angriffe und liefert gleichzeitig positive Rückmeldung für korrekt erkannte Phishing-Simulationen. Der interne IT-Support wird durch unterstützende Informationen und automatisierte Antwortprozesse entlastet. Im Control Panel kann eingesehen werden, wie viele der simulierten Phishing-E-Mails von Benutzer gemeldet wurden.

   Die geltenden technischen Voraussetzungen für die Nutzung des Outlook Add-Ins entnehmen Sie dem Benutzerhandbuch.

f. Die **E-Trainings** vermitteln Benutzern unterhaltsam, anschaulich und verständlich Grundinhalte zu verschiedenen Themen der IT-Sicherheit. In den Trainings liegt der Fokus auf Inhalten, die auch von technischen Laien im Alltag direkt erkannt und umgesetzt werden können. Zu jedem Thema stehen verschiedene Lernmodule, zum Beispiel in Form eines interaktiven E-Trainings, Kurzvideos oder Dokumentes zur Verfügung.

   i. **Interaktive E-Trainings** haben eine Dauer von bis zu 30 Minuten, abhängig von der Komplexität des Themas. Der Fortschritt des Benutzers wird gespeichert, so dass jedes Modul vom Benutzer in einem Stück oder in mehreren Sitzungen bearbeitet werden kann.

   ii. In den **Kurzvideos** wird die Motivation der Lernenden angesprochen, und einzelne Lernziele werden wiederholt und vertieft.

   iii. Zusätzliche weiterführende Dokumente können unterstützende Informationen zu den E-Trainings enthalten, die Ihre Benutzer für den Schnellzugriff abspeichern oder auch ausdrucken können.

   iv. **Refresher-Module** stehen zur Verfügung, um das Wissen der Benutzer aufzufrischen.

   v. Zusätzlich zu den klassischen E-Trainings bietet SAS auch **Quizze** zu bestimmten Themen an, um das Wissen zu testen. E-Training-Inhalte können diese Quizze enthalten, um den Benutzern eine unterhaltsame Möglichkeit zu bieten, ihren eigenen Wissensstand zu überprüfen und Konzepte aufzufrischen, die in Vergessenheit zu geraten drohen.

g. Das **User Panel** fasst die persönlichen Lerninhalte der Benutzer zentral und bequem an einem Ort zusammen. Benutzer werden automatisch eingeloggt und müssen sich keine Zugangsdaten merken. Sie erhalten dort Zugriff auf ihre gebuchten und zugewiesenen E-Trainings und andere Lerninhalte.

   Das User Panel speichert alle Zwischenstände der Trainings und die Benutzer können auch bereits abgeschlossene **Lerninhalte** jederzeit anschauen. Benutzer können außerdem eine **personalisierte Auswertung** über die erhaltenen Phishing-Mails einsehen. Benutzer können über das User Panel ihr Widerspruchsrecht wahrnehmen und flexibel anpassen, sofern sie selbst nicht als Absender von Phishing E-Mails fungieren möchten.

h. Über das **Control Panel** erhalten Administratoren Zugang zu einem **Dashboard**, das ihnen jederzeit Einblick in den aktuellen Stand der Simulations- und Trainingsfortschritte und in das aktuelle Sicherheitsverhalten der Benutzer gibt. Zudem können hier die Konfigurationen für den Security Awareness Service angepasst werden

i. Nach mindestens einem Jahr erfolgreichem Security Awareness Service stellt Hornetsecurity ein **Unternehmenszertifikat** aus, das als Nachweis für das durchgeführte Awareness Training und dessen Ergebnisse dient und bei Audits vorgelegt werden kann. Das Zertifikat wird auf Antrag des Kunden ausgestellt. Es wird jährlich erneuert und ist für ein Jahr gültig.

j. SAS bietet optional einen **Privacy Mode**, der aktiviert werden kann, wenn ausschließlich anonymisierte Ergebnisse und Daten des Awareness Trainings reportet und dargestellt werden sollen, um keine Rückschlüsse auf Einzelergebnisse zu gestatten.

   Personenbezogenes Reporting kann nach lokalem Recht abstimmungsbedürftig oder mitbestimmungspflichtig sein. Wenden Sie sich an Ihren Rechtsbeistand oder Datenschutzbeauftragten. In diesem Fall wird die Verwendung des Privacy Mode empfohlen.

k. Um den Mitarbeiterschutz zu gewährleisten, ist eine spätere Deaktivierung des Privacy Mode nicht möglich.

2. Pflichten des Kunden

   Der Kunde ist verpflichtet, den Service in Übereinstimmung mit der Acceptable Use Policy zu nutzen und auf ihn zuzugreifen und sich an die Fair Use Policy (Richtlinie zur angemessenen Nutzung) zu halten.

3. Einschränkungen und Anforderungen

   Hornetsecurity leistet Support für autorisierte Benutzer, soweit es sich um Hornetsecurity-Systeme handelt. Der Support für die Systeme des Kunden ist nicht Bestandteil des Vertrages. Dazu gehören auch Anwendungen von Drittanbietern, die durch die eigenständige Verarbeitung von URLs und Links Einfluss auf die Service-Statistik haben können.

4. Fair Use Policy (Richtlinie zur angemessenen Nutzung)

   a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Soft-ware erforderlich sind und die wir in diesem Zusammenhang zur Verfügung stellen, werden von allen unseren Kunden gemeinsam genutzt. Daher haben wir das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.

   b. Wir haben uns dazu entschlossen, keine Richtwerte vorab festzulegen, die eine exzessive oder unangemessene Nutzung bestimmen, da wir nach unserem Ermessen entscheiden können, unsere normalen Service-Levels aufrechtzuerhalten, indem wir anderen Nutzern reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zuweisen oder Ressourcen anderweitig skalieren. Sie verstehen, dass wir, wenn wir uns entscheiden, unsere Fair Use Policy nicht aktiv durchzusetzen, nicht davon ausgehen, dass wir auf unser Recht, dies zu tun, verzichtet haben, noch haben wir zugestimmt, dass Sie unsere Dienste weiterhin auf demselben Niveau nutzen, wie Sie es zu einem bestimmten Zeitpunkt tun.

   c. Um unsere Dienste nutzen zu können, müssen Sie abrechenbare Einheiten erwerben. Die Anzahl der abrechenbaren Einheiten, die Sie benötigen, hängt von einer Reihe von Kriterien ab, z. B. von

der Größe Ihres Unternehmens, der Anzahl der Benutzer, usw. Sie können die Anzahl der abrechenbaren Einheiten, die Sie benötigen, anhand unserer Leitfäden, die wir auf unserer Webseite für Gebühren und Abrechnungen hochgeladen haben, oder durch die Unterstützung unseres Vertriebsteams ermitteln.

d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienstleistungen zweckmäßig nutzen, und zwar in einer Weise, die es nicht erforderlich macht, dass wir unverhältnismäßig viele Ressourcen zuweisen müssen. Um dies festzustellen, werden wir Ihre Nutzung unserer Ressourcen (z. B. Speicherbedarf, Anzahl paralleler Verbindungen) mit dem eines durchschnittlichen Kunden vergleichen. Den Durchschnittskunden ermitteln wir, indem wir die 5% höchsten und die 5% niedrigsten Kunden der jeweiligen Ressource unberücksichtigt lassen und den Mittelwert über alle unsere aktiven Kunden bilden.

e. Spezifische Merkmale, die sich auf die Branche beziehen, in der Sie tätig sind, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.

f. Wenn wir nach vernünftigem Ermessen und in gutem Glauben davon ausgehen, dass die Nutzung unserer Lösung durch Sie nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen:

    i. Ihnen erlauben, unsere Lösungen weiterhin zu nutzen, jedoch vorbehaltlich unter der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.

    ii. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieser Zeit werden alle Services und/oder der Betrieb ausgesetzt.

g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:

    i. werden alle Daten (Metadaten, Sicherungsdaten oder andere) am Ende des von uns in der diesbezüglichen Benachrichtigung fest-gelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.

    ii. erhalten Sie eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums.