Handlungsfähige Organisationen brauchen einen zuverlässigen Schutz gegen Cyberangriffe. Der Schlüssel dazu ist eine nachhaltige Sicherheitskultur. Dabei gilt es, alle abzuholen: Von der Führung bis zum einzelnen Mitarbeiter. Denn nachhaltige Sicherheitskultur kann nur gemeinsam erreicht werden.

Der Erste Abschnitt befasst sich mit Fragen zur Durchführung vom Security-Awareness-Training und der Phishing-Simulation sowie allgemeinen Fragen zu unserem Produkt. Im zweiten Abschnitt beantworten wir Fragen rund um das Thema Datenschutz.

Inhalt

FRAGEN ZUR DURCHFÜHRUNG

1. Welche Leistungen umfasst der Security Awareness Service?

Hornetsecurity bietet einen umfassenden Security Awareness Service im Autopiloten, der folgende Leistungen beinhaltet:

- Spear-Phishing-Simulation
- Vollständig automatisierte Steuerung des Awareness-Trainings und der Phishing-Simulation
- E-Learnings, Kurzvideos, Quizze und Auffrischungskurse
- Awareness-Materialien
- Outlook Reporter Button Add-In
- Live-Reporting und Statistiken zum Awareness Training

Der Security Awareness Service wird von Hornetsecurity kontinuierlich weiterentwickelt und an aktuelle Angriffe angepasst. Durch die jeweils didaktisch und fachlich aktuellen Phishing E-Mails und Trainings-Module können sich unsere Kunden darauf verlassen, eine der fortschrittlichsten Plattformen für eine kontinuierliche Durchführung des Awareness-Trainings zu nutzen.

2. Warum eine Phishing-Simulation?

Security Awareness Trainings haben zum Ziel, das Verhalten der Anwender zu verändern und mehr Sicherheit im Unternehmen zu erreichen. Um dies im Alltag zu schaffen, sind viele Trainingsmethoden möglich. Letztlich kommt es jedoch darauf an, dieses Verhalten im Alltag auch nachhaltig beizubehalten. Der Schlüsselbegriff dazu ist Sicherheitskultur.

Eine gute Sicherheitskultur muss das richtige Mindset und Skillset der Anwender stärken, sowie benutzbare und sichere Tools und Prozesse im Unternehmen bieten. Phishing-Simulationen prägen das Mindset und Skillset der Anwender nachhaltig, um ein sicheres Verhalten zu bewirken. In Kombination mit einem Reporter Button können darüber hinaus einfache und zuverlässige Prozesse umgesetzt werden, wodurch Mitarbeiter Phishing-Mails melden können und damit ein sicheres Verhalten im Alltag verankern.

Dabei ist klar: Phishing-Simulationen dürfen nicht das einzige Trainingsmittel sein. Das Mindset, Skillset und Toolset muss über verschiedene Kanäle geschärft werden. Dazu gehört ein Trainingskonzept, das neben Phishing-Simulationen auch E-Learning, Kurzvideos und Awareness-Materialien bietet. Der richtige Einsatz der Stärken und Vorzüge der verschiedenen Maßnahmen sorgt dafür, dass ein Awareness Training erfolgreich wird.

3. Wie funktioniert der Security Awareness Service?

Pro Teilnehmer werden 2 bis 3 Spear-Phishing E-Mails pro Monat zu einem zufälligen Zeitpunkt versendet. Diese Mails bilden verschiedene Schwierigkeitsgrade ab, die sich an der Vorbereitungszeit eines Angreifers orientieren, welche er für einen vergleichbaren Angriff aufbringen müsste. Das Schwierigkeitslevel steigt dabei über die Zeit, abhängig davon, wie gut ein Teilnehmer auf die bisherigen Phishing E-Mails reagiert hat.

Abhängig vom aktuellen ESI® wird für jeden Teilnehmer entschieden, ob weitere Trainingsmaßnahmen, wie bspw. E-Learning Module oder Kurzvideos angestoßen werden sollen. Erreicht ein Teilnehmer ein bestimmtes ESI®-Niveau, werden die Trainingsmaßnahmen pausiert oder auf eine E-Mail pro Monat reduziert, bevor erneut gemessen wird, ob das Sicherheitsverhalten noch dem erreichten ESI®-Niveau entspricht oder drüber liegt. Ist das nicht der Fall, werden weitere Trainingsmaßnahmen eingeleitet.

Werden die Inhalte aus der Phishing-Mail von einem Teilnehmer geöffnet, so wird er auf eine Erklärseite mit konkreten Hinweisen und Erklärungen weitergeleitet. So lernen die Teilnehmer interaktiv, wie sie in Zukunft Phishing-Mails erkennen können.

4. Wie funktioniert der ESI®?

Mit Hornetsecurity steht ein Anbieter von Security-Awareness-Trainings zur Verfügung, der Trainings-Inhalte, -Methoden und -Werkzeuge zu einem innovativen Service-Angebot kombiniert. Zentrales Alleinstellungsmerkmal ist der patentierte Employee Security Index (ESI®) von IT-Seal, die seit Mai 2022 zur Hornetsecurity-Gruppe gehört. Damit steht ein wissenschaftlich fundierter Benchmark zur Verfügung, mit dem sich das Sicherheitsverhalten von Mitarbeitern objektiv messen und überwachen lässt.

Dies ist mit den bisherigen Messansätzen nicht möglich, da sie keine Standardisierung – und damit keine Vergleichbarkeit über längere Zeiträume hinweg oder zwischen verschiedenen Abteilungen, Rollen und Unternehmensstandorten erlauben. Damit verbunden ist das Risiko, dass einzelne Sicherheitsprobleme, Fehler oder Klicks auf Spear-Phishing-Mails überbewertet oder unterbewertet werden und die Unternehmen letztlich keine Transparenz über das Sicherheitsverhalten ihrer Mitarbeiter erhalten. Sie investieren daher häufig zu viel oder auch zu wenig, um ein angemessenes Sicherheitsniveau zu erreichen.

Vorbereitungszeit entscheidend

Anders der ESI®, der eine realitätsnahe und reproduzierbare Methode zur Messung der Security Awareness darstellt. Zur Berechnung des ESI® werden die Spear-Phishing-Angriffe in unterschiedliche Kategorien (sogenannte „Level“) unterteilt, die sich nach dem Zeitaufwand richten, die Cyberkriminelle in die Vorbereitung und Durchführung investieren müssen. Dieser Aufwand setzt sich unter anderem aus der Informationsbeschaffung aus öffentlich zugänglichen Quellen, der technischen Vorbereitung, dem Kopieren von Webseiten-Designs

sowie der Bereithaltung der für einen Phishing-Angriff notwendigen IT-Infrastruktur zusammen. So lassen sich sieben Kategorien einteilen, die jeweils einer Vorbereitungszeit von einer Stunde bis mehrere Tage und Wochen entsprechen. Der individuelle ESI® eines Unternehmens ergibt sich daraus, wie die Beschäftigten auf Phishing-Simulationen verschiedener Schwierigkeitsgrade reagieren.

Um das Sicherheitsniveau eines Unternehmens standardisiert einordnen zu können, hat Hornetsecurity Toleranzwerte für ein vorbildliches Sicherheitsverhalten der Testgruppen definiert. Diese Werte basieren auf den „Erfolgsraten" aus Sicht der Angreifer. Da „Erfolgsraten" von 0 illusorisch sind (jeder Mensch macht Fehler), liegen die Toleranzwerte jeweils an der Schnittstelle zwischen Sicherheit und Realisierbarkeit. Eine vorbildliche Testgruppe mit den niedrigsten „Erfolgsraten" erreicht auf einer Skala von 0 – 100 mindestens einen ESI® von 90. Wird doppelt so häufig kritisches Verhalten gezeigt, erreicht die Gruppe einen ESI®-Wert von lediglich 80; bei dreifach kritischem Verhalten nur noch einen ESI® von 70. Ergebnisse unter 70 gelten als kritisch. Die von Hornetsecurity definierten Toleranzwerte basieren auf dem aktuellen Stand der Forschung und Erfahrungswerten mit Phishing-Simulationen in Unternehmen verschiedenster Branchen.

Damit bietet der ESI® den Unternehmen eine greifbare und verlässliche Kennzahl, um die einzelnen Mitarbeitergruppen standardisiert miteinander zu vergleichen. Wer ist sicherer, der Vertrieb oder die Personalabteilung, und wie steht die Geschäftsführung im Vergleich zur Buchhaltung da? Diese Informationen sind wertvoll, wenn es um die gezielte Ableitung weiterer Schulungsmaßnahmen geht.

5. Welche Vorbereitungen müssen getroffen werden, damit die Phishing-Simulation nicht vom Spam-Filter abgefangen wird?

Für den Security Awareness Service muss ein Whitelisting durchgeführt werden, damit die Phishing-Mails nicht im Spam-Filter landen. Für Endkunden, die bereits einen Service der 365 Total Protection-Familie von Hornetsecurity nutzen, wird das **Whitelisting automatisch** durchgeführt.

Für alle anderen Kunden muss das Whitelisting manuell durchgeführt werden. Ein „How-to" und Details zum Whitelisting finden Sie in unserem Handbuch unter dem Punkt "Erweiterte Zustellung für Microsoft 365 Defender einrichten".

6. Wie funktioniert die Auswertung?

Das Sicherheitsverhalten (Klick- und Meldeverhalten auf simulierte Phishing E-Mails) der Gruppen und einzelnen Teilnehmer werden für die Auswertung im Employee Security Index (ESI®) verrechnet. Im Awareness Dashboard im Control Panel werden dazu verschiedene Statistiken in Echtzeit bereitgestellt, die u. a. auch den aktuellen ESI® auf Unternehmens-,

Gruppen- und Teilnehmer-Ebene zeigen. Dadurch wird die Security Awareness messbar und das derzeitige Gefährdungsrisiko sichtbar.

Im Control Panel kann der „Privacy Mode" konfiguriert werden. Ist dieser aktiviert, sind keine Einzelergebnisse der Teilnehmer einsehbar. In diesem Fall sollte auch darauf geachtet werden, dass Gruppen mit mindestens 10 Mitarbeitern gebildet werden. Nur so kann gewährleistet werden, dass keine Rückschlüsse auf einzelne Teilnehmer mehr möglich sind.

7. Was ist bei der Auswahl der Teilnehmer zu beachten?

Grundsätzlich sollten alle Mitarbeiter am Security Awareness Training teilnehmen, die über einen E-Mail-Account im Unternehmen verfügen. Dabei spielen Mitarbeiterposition und Standorte keine Rolle.

8. Wird die Phishing-Simulation und das E-Learning auch in anderen Sprachen angeboten?

Ja, sowohl die Phishing Simulation als auch die E-Learnings und anderen Lerninhalte werden in mehreren verschiedenen Sprachen angeboten. Welche Sprachen das sind, geht aus unserer aktuellen E-Learning-Broschüre hervor.

9. Sollten die Mitarbeiter vor Beginn des Security Awareness Trainings bzw. der Phishing-Simulation informiert werden?

Unsere Erfahrung zeigt: eine vorherige Ankündigung wirkt sich positiv auf die Akzeptanz der Mitarbeiter aus. Die Phishing-Simulation wirkt dadurch vielmehr wie eine gemeinsame Trainingsmaßnahme zur Verbesserung der Security Awareness im Unternehmen. Die Mitarbeiter fühlen sich dadurch nicht ausgetrickst. Zudem hat die Vorankündigung keinen signifikanten Einfluss auf das Ergebnis. Zwei Wochen zwischen Ankündigung und Start der Phishing-Simulation gibt außerdem ausreichend Zeit, dass die meisten Mitarbeiter die Ankündigung bereits wieder vergessen haben.

10. Dürfen Mitarbeiter ihre Teilnahme an der Phishing-Simulation verweigern?

Grundsätzlich werden Unternehmen von verschiedenen Seiten her dazu angehalten, regelmäßig Maßnahmen zur technischen und organisatorischen Sicherheit zu treffen. Dazu gehören auch Schulungen der Mitarbeiter zu IT-Sicherheitsthemen. Die Durchführung von kontinuierlichen Security Awareness Trainings und Phishing-Simulationen haben sich dabei als ein besonders wirksames Instrument erwiesen, um das Sicherheitsverhalten der Mitarbeiter der verschärften Cyber-Bedrohungslage der heutigen Zeit anzupassen und in der gesamten Organisation eine nachhaltig gelebte Sicherheitskultur zu etablieren. Vor diesem Hintergrund dürfen sich

Mitarbeiter nicht den Schulungsmaßnahmen verweigern, wenn diese vom Unternehmen vorgeschrieben sind.

Dabei gilt es aber einen wichtigen Aspekt zu beachten, denn manche Regulierungen lassen Phishing-Simulationen generell nur dann zu, wenn sie verhältnismäßig sind und nicht zu weit in das Persönlichkeitsrecht eingreifen.

In diesen Fällen empfehlen wir, den Privacy Mode zu aktivieren, wodurch die einzelnen Teilnehmer-Ergebnisse nur anonymisiert ausgewertet werden und somit keine Rückschlüsse mehr auf die einzelnen Personen mehr möglich sind.

Für jeden einzelnen Teilnehmer besteht zudem die Möglichkeit, ein Widerspruchsrecht wahrzunehmen, damit keine Phishing-Simulationen in seinem Namen versendet werden. Das Widerspruchsrecht kann von jedem Mitarbeiter selbst im Security Hub – der Lernplattform – eingestellt werden. Den Mitarbeitern sollte aber im Voraus klar kommuniziert werden, dass dies kein Widerspruchsrecht darstellt, an der Phishing-Simulation teilzunehmen.

Als eine gute Vorgehensweise hat sich erwiesen, die Mitarbeiter im Vorfeld aufzuklären, warum der Versand von simulierten Phishings-Mails unter ihren Namen sinnvoll ist: Denn es gibt Angriffsarten, bei denen sich Hacker als Kollegen ausgeben, um vertrauensvoll zu wirken. Wenn die Mitarbeiter verstehen, dass der Versand von Phishing-Mails unter ihren Namen dazu dient, um diese Art von Angriffsarten zu simulieren, haben sie eine gute Entscheidungsgrundlage, um über die Ausübung ihres Widerspruchsrechtes nachzudenken.

FRAGEN ZUM DATENSCHUTZ

11. Dürfen Mitarbeiterdaten an Hornetsecurity übertragen werden?

Die Übermittlung und Verwendung der Daten sind gestattet, wenn ein berechtigtes Arbeitgeberinteresse vorliegt und schutzwürdige Interessen des betroffenen Arbeitnehmers nicht entgegenstehen. Daher sollte der Arbeitgeber keine intern bekannten Daten übermitteln, die ein „echter" Angreifer nicht ohne Weiteres erfahren könnte. Zudem muss eine Vereinbarung zur Auftragsdatenverarbeitung geschlossen werden.

12. Muss ich vor Weitergabe der Daten die Zustimmung des Betriebsrats / Personalrats einholen?

Nein. Die Zustimmung des Betriebsrats oder Personalrats ist nicht notwendig. Allerdings muss er informiert werden, damit er die Einhaltung der Datenschutzvorschriften überprüfen kann. Wir empfehlen den Betriebsrat möglichst früh einzubinden. So wird sichergestellt, dass alle Parteien mit dem Vorgehen einverstanden sind.

13. Wo findet die Datenverarbeitung statt?

Die Datenverarbeitung findet rechtskonform in eigenen, redundant ausgelegten Hochsicherheits-Datenzentren in den verschiedenen Regionen statt, in denen Hornetsecurity seine Services anbietet und wo die größte Nähe zum Kunden besteht.

Für die DACH-Region: Deutschland

Weitere Standorte der redundant ausgelegten Datenzentren-Standorte sind:

- UK
- Spanien
- USA
- Canada
- Australien

14. Welche Mitarbeiterdaten werden zur Durchführung des Awareness Trainings und der Phishing-Simulation benötigt?

Benötigt werden: Namen, E-Mailadressen, Sprache der Teilnehmer, Gruppezuordnung, Abteilung und Position. Den Namen benötigen wir, damit wir die Teilnehmer korrekt ansprechen können. Die E-Mailadresse, um die Teilnehmer kontaktieren zu können. Die Sprache ermöglicht es uns, den Teilnehmern die Inhalte in der richtigen Sprache anzeigen zu können. Die Gruppenzuordnung legt fest, in welche Gruppe das Klickverhalten der Teilnehmer für die Gruppenauswertung im Dashboard einfließt. Die Abteilung und Position nutzen wir, um zielgerichtete Spear-Phishing-Mails versenden zu können.

15. Werden darüber hinaus noch weitere Daten gesammelt?

Darüber hinaus werden zudem Daten zu Nutzerreaktionen gesammelt. Dazu zählen wir, ob Mitarbeiter auf gefälschte Links geklickt haben, oder ob Nutzerdaten auf einer präparierten Website eingegeben wurden – die Inhalte dieser Dateneingabe werden nicht übertragen. Zudem werden alle Daten abstrahiert (pseudonymisiert) gespeichert.

16. Wie wird der Schutz der personenbezogenen Daten sichergestellt?

Das Thema Datenschutz hat für uns eine hohe Priorität. Jegliche personenbezogenen Daten werden bei uns separat gespeichert, sodass wir mit pseudonymisierten Daten arbeiten. Lediglich zum E-Mail-Versand werden über die Pseudonyme aus den separaten Datenbanken auf personenbezogene Daten wie Namen oder E-Mail-Adresse zugegriffen. Diese separaten Datenbanken werden nach Beendigung des Service in Absprache sofort gelöscht. Darüber hinaus geben wir keine mitarbeiterbezogenen Informationen an Dritte heraus.

17. Wie werden datenschutzrechtlichen Anforderungen der DSGVO eingehalten?

Hornetsecurity kontrolliert und überarbeitet regelmäßig das Datenschutzkonzept und die umgesetzten Maßnahmen.

Zudem führt der Datenschutzbeauftragte von Hornetsecurity regelmäßig angekündigte sowie unangekündigt Kontrollen und Audits durch. Bei Bedarf kann eine entsprechende Bestätigung zur Verfügung gestellt werden.

18. Wie nehme ich Kontakt zum Datenschutzbeauftragten auf?

Datenschutzbeauftragter ist: Lukas Wagner, LL.M.

Kontakt über: datenschutz@hornetsecurity.com