Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

KOMMUNIKATIONSENTWÜRFE IM RAHMEN DES SECUREPOINT AWARENESS PLUS BUILDINGS

BESCHREIBUNG

Dieses Dokument beinhaltet Kommunikationsentwürfe, die Sie für Ihre interne Kommunikation im Rahmen des Securepoint Cyber Security Awareness-Trainings nutzen können. Die Verwendung ist in Ihrer beauftragten Leistung enthalten. Nehmen Sie gerne Anpassungen an den Texten vor, um diese bestmöglich für Ihre Organisation zu individualisieren.

Wir empfehlen insbesondere die Vorankündigung der Phishing-Simulation an alle Mitarbeitenden durchzuführen. Dies hat – unserer Erfahrung nach – überwiegend positive Effekte zur Folge:

Chancen:

- Rechtzeitige Einbindung aller Entscheider – niemand wird überrascht
- Steigerung der Awareness bereits vor Beginn der Phishing-Simulation
- Deutliche Wahrnehmung des Mehrwerts der Phishing-Simulation
- Positive Anerkennung der Cyber Security Awareness als *nützlich* statt *lästig*

Risiken:

- Kein reiner Blindtest – leicht geringerer Initialwert der Klickrate

Die Kommunikationsentwürfe für Ihre/n Datenschutzbeauftragte/n, Ihren IT-Support und die Vorankündigung an Ihre Mitarbeitenden, empfehlen wir vor Beginn der Maßnahme zu nutzen.

Die Zwischenkommunikation 1 können Sie heranziehen um erste Ergebnisse nach Abschluss der ersten zwei Wochen („Initialphase“) mit Ihren Mitarbeitenden zu teilen. Die Zwischenkommunikation 2 können Sie nach Belieben verwenden, um Ihre Mitarbeitenden über den aktuellen Stand der Simulation zu informieren und die Sichtbarkeit des Themas in Ihrem Unternehmen hochzuhalten. Wir empfehlen Ihnen, die Awareness-Maßnahme über die ganze Laufzeit proaktiv zu kommunizieren.

Das vorliegende Dokument soll Sie dabei unterstützen, die verschiedenen Schritte in der Vorbereitung und während der Durchführung intern zu kommunizieren.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Die Abschlussauswertung können Sie jeweils zum Ende eines Simulationsjahres versenden, um die Auswertung zu teilen und die Fortsetzung anzukündigen.
Am Ende des Dokumentes finden Sie zusätzlich eine Übersicht aller System-Mails, die von Awareness PLUS versendet werden können.

INHALTSVERZEICHNIS

Kommunikationsentwürfe im Rahmen des Awareness Buildings 1

Beschreibung 1

Übersicht Projektverlauf und Kommunikationspunkte 3

Entwurf Datenschutzbeauftragte/r 4

Entwurf IT-Support 5

Entwurf Vorankündigung Mitarbeitende 7

Entwurf Zwischenkommunikation Mitarbeitende 1 9

Entwurf Zwischenkommunikation Mitarbeitende 2 11

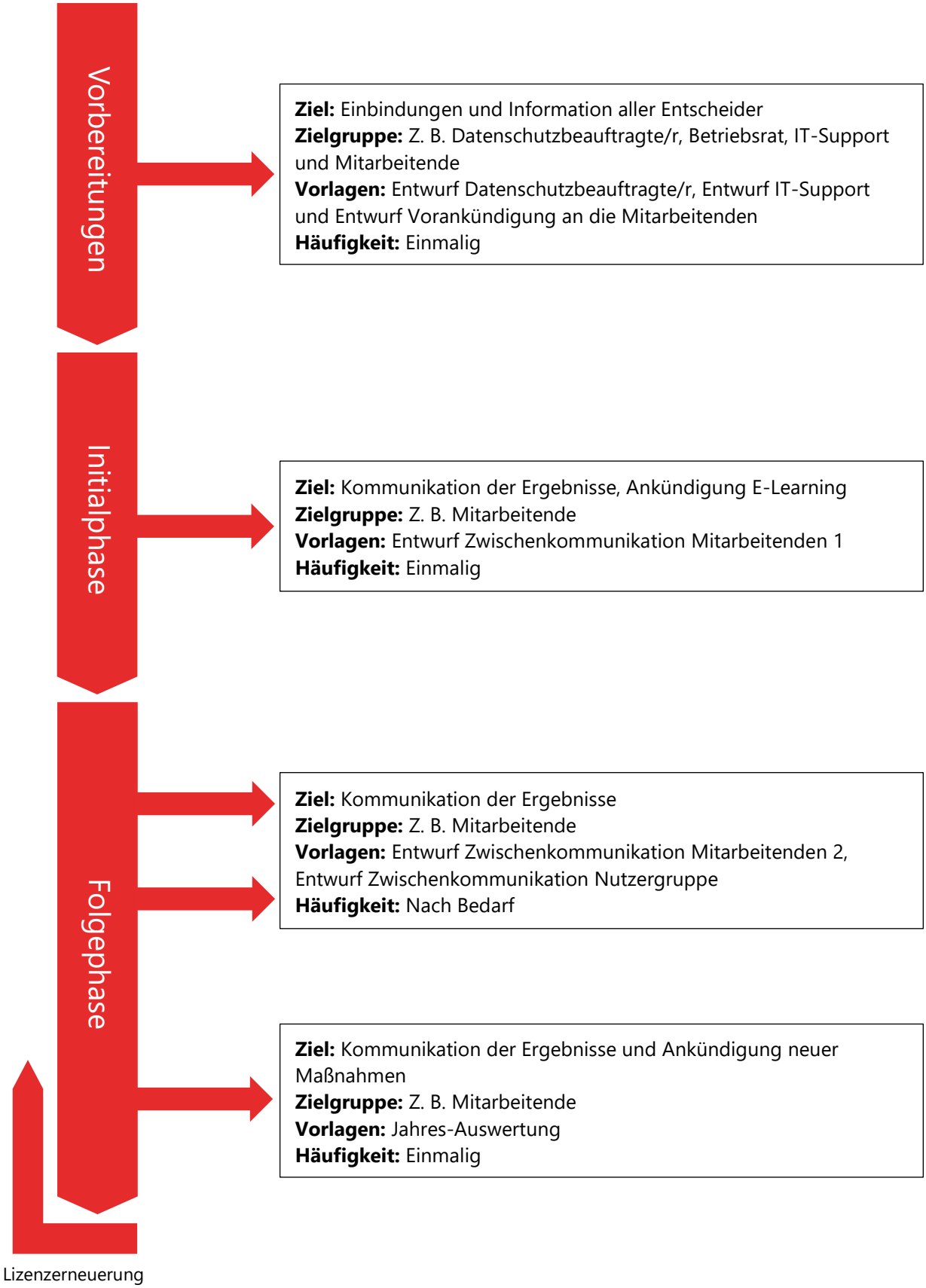
Jahres-Auswertung 13

Allgemeiner Hinweis:

Alle gelb markierten Satzteile sind ggf. spezifisch von Ihnen an die zutreffenden Umstände anzupassen. Zusätzlich in **< Klammern gesetzte Bestandteile >** deuten darauf hin, dass die darauffolgende Textpassage in manchen Fällen nicht zutrifft und somit von Ihnen aus dem Schriftstück entnommen werden sollte.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

ÜBERSICHT PROJEKTVERLAUF UND KOMMUNIKATIONSPUNKTE



Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

ENTWURF DATENSCHUTZBEAUFTRAGTE/R

Betreff: Information zum Awareness PLUS-Training und Bitte um Freigabe

Sehr geehrte/r Herr/Frau ...,

anbei übersende ich Ihnen vorab zur Information eine Übersicht für eine Trainingsmaßnahme zur Steigerung unserer Cyber Security Awareness. Zielsetzung ist:

- Transparente Einschätzung der aktuellen Anfälligkeit für Phishing-Angriffe
- Schulung unserer Mitarbeitenden durch simulierte Phishing-Angriffe
- Minimierung des Risikos von Cyber-Angriffen für unser Unternehmen

Das Training beinhaltet als Kernelement eine 12-monatige Simulation von Phishing- Angriffen durch vorbereitete E-Mails. Insgesamt erhält jeder Mitarbeitende in diesem Zeitraum bis zu 12 solcher E-Mails. Diese E-Mails sind ungefährlich und die enthaltenen Links führen unsere Mitarbeitenden lediglich auf interaktive Lernseiten. Zu keiner Zeit besteht ein Sicherheitsrisiko für die Geräte oder Daten unserer Mitarbeitenden.

Die Durchführung der Simulation sowie die Verarbeitung der E-Mail-Adressen und personenbezogenen Daten (Name etc.) unserer Mitarbeitenden erfolgt durch unseren Dienstleister Securepoint GmbH datenschutzkonform gemäß beiliegendem Vertrag zur auftragsbezogenen Verarbeitung personenbezogener Daten.

Die Phishing-Simulation ist als Schulungsangebot an unsere Mitarbeitenden zu verstehen – keinesfalls geht es uns darum einzelne Mitarbeitende „vorzuführen". Selbstverständlich erfolgt die Simulation anonym. Es sind demnach keine Rückschlüsse auf einzelne Mitarbeitende möglich. Stattdessen werden lediglich aggregierte, übergreifende Zahlen über alle Mitarbeitenden erfasst, z. B.:

- Öffnungsrate der jeweiligen Phishing-E-Mails
- Klickrate auf Phishing-Links innerhalb dieser E-Mails
- Klickraten im Zeitverlauf

Bei weiteren Fragen kommen Sie gerne auf mich zu.

Mit freundlichen Grüßen

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

ENTWURF IT-SUPPORT

Betreff: Information zum anstehenden Cyber Security Awareness PLUS-Training

Sehr geehrte/r Herr/Frau …,

anbei übersende ich Ihnen vorab zur Information eine Übersicht für eine Trainingsmaßnahme zur Steigerung unserer Cyber Security Awareness. Zielsetzung ist:

- Erlangung von Transparenz über aktuelle Anfälligkeit für Phishing-Angriffe
- Schulung unserer Mitarbeitenden durch simulierte Phishing-Angriffe
- Minimierung des Risikos von Cyber-Angriffen für unser Unternehmen

Das Training beinhaltet als Kernelement eine 12-monatige Simulation von Phishing- Angriffen durch vorbereitete E-Mails. Insgesamt erhält jeder Mitarbeitende in diesem Zeitraum bis zu 12 solcher E-Mails. Diese E-Mails sind ungefährlich und die enthaltenen Links führen unsere Mitarbeitende lediglich auf interaktive Lernseiten. Zu keiner Zeit besteht ein Sicherheitsrisiko für die Geräte oder Daten unserer Mitarbeitenden. Zur entsprechenden Auftragsverarbeitungs-Vereinbarung mit dem Dienstleister Securepoint GmbH bin ich bereits in Abstimmung mit unserem Datenschutzbeauftragten.

Die Absenderadressen und Betreffzeilen der E-Mails an unsere Mitarbeitenden können Sie der beigefügten Übersicht entnehmen. Viele unserer Mitarbeitenden werden diese E-Mails hoffentlich als Phishing-Versuche erkennen und bei Ihnen melden. Ich empfehle hierfür bereits ein gesondertes Routing dieser Tickets einzurichten. Optimal wäre, wenn Sie mir die Anzahl der gemeldeten E-Mails (bezogen auf die o. g. E-Mails) in einem kurzen monatlichen Reporting zur Verfügung stellen könnten.

Bitte behandeln Sie die Liste der Templates vertraulich. Um einen maximalen Schulungseffekt zu erzielen, erfahren die Kollegen keine Details zu den kommenden E-Mails.

Um die Maßnahme technisch zu ermöglichen, bitte ich Sie, die Absenderadressen unseres Dienstleisters Securepoint in unser Whitelisting aufzunehmen:

- *< Bitte entnehmen Sie die IP-Adressen dem Awareness PLUS Portal unter ‚Whitelisting' >*

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Weitere technische Informationen von Awareness PLUS finden Sie unter https://wiki.securepoint.de/AwarenessPLUS. Geben Sie mir doch bitte eine kurze Rückmeldung, sobald das Whitelisting erfolgt ist, und kommen Sie bei weiteren Fragen gerne auf mich zu.

Mit freundlichen Grüßen

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

ENTWURF VORANKÜNDIGUNG MITARBEITENDE

Betreff: Information zum anstehenden Cyber Security Awareness PLUS-Training

Liebe Kolleginnen, liebe Kollegen,

wir alle kennen es aus der Presse: Cyber-Angriffe im privaten wie im beruflichen Kontext nehmen stetig zu. Zur Steigerung unserer Abwehrfähigkeit gegen solche Angriffe führen wir bald ein Cyber Security Awareness-Training durch. Ziele sind:

- Erlangung von Transparenz über aktuelle Anfälligkeit für Phishing-Angriffe
- Schulung unserer Mitarbeitenden durch simulierte Phishing-Angriffe
- Minimierung des Risikos von Cyber-Angriffen für unser Unternehmen

Das Training beinhaltet als Kernelement eine 12-monatige Simulation von Phishing- Angriffen durch vorbereitete E-Mails. Insgesamt erhält jeder von Ihnen in diesem Zeitraum bis zu **12** solcher E-Mails **– im Durchschnitt also etwa eine E-Mail pro Monat**. Diese E-Mails sind ungefährlich und die enthaltenen Links führen Sie lediglich auf interaktive Lernseiten. Dennoch ist Vorsicht geboten, da auch jederzeit **echte** Angriffsversuche per Phishing-Mails erfolgen können. Bitte nehmen Sie diese Gefahr sehr ernst, und **klicken Sie keinesfalls** auf verdächtige bzw. unbekannte Links oder Anhänge. Sollten Sie eine E-Mail als (simulierten) Phishing-Versuch vermuten, dann leiten Sie diese an unseren IT-Support weiter.

Falls Sie den simulierten Phishing-Versuch nicht erkannt und angeklickt haben, werden Sie auf eine Lernseite weitergeleitet. Bitte nehmen Sie sich die Zeit die Hinweistexte durchzulesen, um zu lernen, woran Sie Phishing-Mails erkennen können. Dadurch wird das Risiko eines Cyberangriffs auf unser Unternehmen deutlich reduziert. Ein Beispiel für die Lernseiten sehen Sie hier im Bild.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Zu keiner Zeit besteht ein Sicherheitsrisiko für Ihre Geräte oder Ihre Daten. Selbstverständlich erfolgt die Simulation komplett anonym. Weder wir noch der Dienstleister Securepoint (https://www.securepoint.de/), der die Simulation für uns durchführt, kann zu irgendeinem Zeitpunkt sehen, wie Sie persönlich klicken oder sich verhalten. Wir erhalten von Securepoint lediglich eine aggregierte, zusammenfassende Übersicht.

< Bei E-Learning als Bestandteil der Awareness-Maßnahme >

Ergänzend zu der Phishing-Simulation bekommen Sie bald Zugriff auf ein spezielles E-Learning-Angebot. Hier sind E-Learning-Module verfügbar, die jeweils mit einem spannenden Quiz versehen sind. Das erworbene Wissen ist auch für den privaten Kontext sehr wertvoll!
Bitte helfen Sie mit, uns alle sicherer gegen Cyber-Angriffe zu machen! Bei Fragen können Sie sich jederzeit gerne an mich wenden.

Mit freundlichen Grüßen

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

ENTWURF ZWISCHENKOMMUNIKATION MITARBEITENDE 1

Betreff: Information zum laufenden Cyber Security Awareness PLUS-Training

Liebe Kolleginnen und Kollegen,

wie viele von Ihnen sicherlich mitbekommen haben, haben wir in den letzten Wochen eine etwas andere Art der Sensibilisierung für das Thema IT-Sicherheit bzw. den sicheren Umgang mit E-Mails durchgeführt.

Phishing-Simulation

Im Rahmen einer Phishing-Simulation mit dem Sicherheitsunternehmen Securepoint GmbH haben Sie alle einige E-Mails erhalten, die realistischen Phishing-Angriffen auf unser Unternehmen nachempfunden waren. Zusätzliche Informationen zu einer solchen Simulation können Sie in einer Zusammenstellung der häufigsten Fragen unter https://wiki.securepoint.de/AwarenessPLUS erfahren. Diejenigen von Ihnen, die auf die entsprechenden Links in den E-Mails geklickt haben, konnten sich ja bereits über die detaillierten Lernseiten darüber informieren, wie man Phishing-Mails erkennt und mit ihnen umgeht.

Für diejenigen, die auf keine der Phishing-Mails geklickt haben, haben wir hier auch noch einmal die Links zu den entsprechenden Lernseiten aufgelistet:

- ...

Insgesamt hatten wir eine **Klickrate von XX %** auf die Phishing-Links.

< Bei E-Learning als Bestandteil der Awareness-Maßnahme >

E-Learning

Während die Phishing-Simulation auch in den nächsten Monaten (mit verringerter Intensität) weiterlaufen wird, haben Sie **ab dem xx.xx.xxxx** die Gelegenheit, Ihr Wissen zum Thema Cyber Security und Phishing zu vertiefen. Dazu bieten wir Ihnen den Zugang zu speziellen E-Learning-

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Modulen an. Diese sind sehr kompakt gehalten und beinhalten jeweils ein spannendes Quiz am Ende, mit dem Sie Ihren Wissensstand durch Ihren persönlichen *SafeScore* ermitteln können. Mit dem Start des E-Learnings erhalten Sie von Securepoint GmbH (noreply@awareness.securepoint.de) eine Einladungsmail zur Registrierung.

Wir hoffen, Ihnen so eine abwechslungsreiche Lernerfahrung zu bieten. Die E-Learnings sind sehr praxisnah und so ausgerichtet, dass Sie die Kenntnisse auch im privaten Kontext verwenden können. Sie enthalten kurze Videos – nutzen Sie also gerne Ihre Lautsprecher/Kopfhörer, falls vorhanden. Sie können die Module aber auch ohne Ton absolvieren. Bei Problemen mit der Lernplattform von Securepoint wenden Sie sich gerne auch an: https://wiki.securepoint.de/AwarenessPLUS.

Ich wünsche Ihnen viel Spaß und weiterhin erhöhte Wachsamkeit!

Viele Grüße

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

ENTWURF ZWISCHENKOMMUNIKATION MITARBEITENDE 2

Betreff: Rückmeldung zum laufenden Cyber Security Awareness-Training

Liebe Kolleginnen und Kollegen,

wie Sie mittlerweile alle wissen, führen wir seit einiger Zeit eine Phishing-Simulation mit dem Sicherheitsunternehmen Securepoint GmbH durch. Diese läuft bei uns im Hause seit mittlerweile X Monaten und jeder von Ihnen wird bereits Kontakt mit den versendeten E-Mails gehabt haben.

Wir möchten uns heute noch einmal an Sie wenden, um Sie über den momentanen Zwischenstand zu informieren.

Die Klickrate beträgt zurzeit X %, das ist gegenüber der letzten Kommunikation eine Verbesserung/Verschlechterung um X %.

< Im Falle einer Verbesserung: >

Wir möchten Ihnen daher an dieser Stelle ein ausdrückliches Lob aussprechen, dass Sie mit ihren E-Mails so verantwortungsbewusst und aufmerksam umgehen. Sie tragen auf diese Art und Weise aktiv zu der Sicherheit unseres Unternehmens bei.

Bitte bleiben Sie weiter aufmerksam und überprüfen Sie alle E-Mails, die Ihnen verdächtig erscheinen, unabhängig davon, ob Sie aus der Simulation stammen oder nicht. IT-Sicherheit geht uns alle an!

< Im Falle einer Verschlechterung: >

Leider haben sich die Werte in der laufenden Maßnahme verschlechtert. Wir möchten Sie daher bitten, diese Simulation mit dem gleichen Ernst zu behandeln wie echte Phishing-Angriffe. Die Schäden eines erfolgreichen Phishing-Angriffs gehen im Normalfall in die Millionen und wir zählen auch auf Ihre Mithilfe, um den Ernstfall zu vermeiden.

< Bei E-Learning als Bestandteil der Awareness-Maßnahme >

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Daher möchten wir Sie an dieser Stelle noch einmal auf das E-Learning der Firma Securepoint hinweisen. Dieses hilft Ihnen sich bestmöglich auf etwaige Cyber-Angriffe vorzubereiten und den richtigen Umgang damit zu trainieren. Falls noch nicht geschehen, registrieren Sie sich am besten noch heute unter https://awareness.securepoint.cloud/register.

IT-Sicherheit geht uns alle an!

Viele Grüße

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

JAHRES-AUSWERTUNG

Betreff: Finale Auswertung der laufenden Awareness-Maßnahme

Liebe Kolleginnen und Kollegen,

zum Abschluss der laufenden Maßnahme möchten wir uns bei Ihnen mit einer kurzen Auswertung melden.

Zu Beginn der Phishing-Simulation haben wir eine Klickrate von X % erzielt, nachdem wir diese nun abschließen, beträgt unsere Klickrate momentan X %. Das entspricht insgesamt einer Reduktion um X % und sind insgesamt X Klicks. Dazu möchten wir Sie alle herzlich beglückwünschen.

Auch bei der sehr wichtigen Interaktionsrate, die z.B. das Aktivieren von Makros oder das Eingeben von Login-Daten dokumentiert, haben wir eine Reduktion erzielt. Zu Beginn der Maßnahme lag diese bei X %, aktuell liegt sie bei X %.

Wir möchten Ihnen zu den erreichten Verbesserungen gratulieren aber an dieser Stelle auch noch einmal darauf hinweisen, dass es an folgenden Stellen aber auch noch Verbesserungsbedarf gibt:

- ...

Für diejenigen, die auf keine oder nur wenige der Phishing-Mails geklickt haben, listen wir hier auch noch einmal die Links zu den entsprechenden Lernseiten auf. Bitte nehmen Sie sich die Zeit, die Hinweise zu den einzelnen E-Mails noch einmal in Ruhe durchzugehen:

- ...

Um unsere Cyber-Sicherheit weiter hochzuhalten und das Sicherheitsbewusstsein aller Mitarbeitenden kontinuierlich noch weiter zu schärfen, werden wir die Simulation in Kürze mit neuen/weiteren E-Mails und E-Learning-Modulen weiterführen.

Viele Grüße