www.security-insider.de

SECURITY INSIDER

Security Awareness Training mit Hoxhunt

Status Quo der Security Awareness
Sicherheitsbewusstsein auf allen Ebenen wecken
Security Awareness Training in der Praxis

Powered by:

HOXHUNT

Das Sicherheitsbewusstsein muss auf allen Ebenen geweckt werden

Cyberrisiken stehen auf der Agenda der Unternehmen weit oben, IT-Sicherheitsvorfälle füllen die Schlagzeilen der Medien. Trotzdem wäre es verfehlt, das Bewusstsein für IT-Sicherheit und damit die Security Awareness als ausreichend oder gar zufriedenstellend anzusehen. Ein Blick auf die aktuelle Sensibilisierung in Security-Belangen deckt viele Lücken auf.

Größte Sorge der Unternehmen, aber mangelndes Bewusstsein für Cyberrisiken

Auf den ersten Blick ist es eine gute Nachricht für Security-Verantwortliche: Cybergefahren sind im Jahr 2022 die größte Sorge für Unternehmen weltweit, so das Allianz Risk Barometer 2022. Die Bedrohung durch Ransomware-Angriffe, Datenschutzverletzungen oder IT-Ausfälle beunruhigt die Unternehmen sogar noch mehr als Geschäfts- und Lieferkettenunterbrechungen, Naturkatastrophen oder die Covid-19-Pandemie, die alle Unternehmen im vergangenen Jahr stark beeinträchtigt haben. Der Hauptgrund dafür ist die Zunahme von Ransomware-Angriffen, die von den Umfrageteilnehmern (57 Prozent) als die größte Cyberbedrohung für das kommende Jahr bewertet wurde. Die Befragten erkennen an, dass es notwendig ist, Sicherheitsvorkehrungen zu verbessern und für künftige Ausfälle zu planen, da sie sonst mit den zunehmenden Konsequenzen seitens der Regulierungsbehörden, Investoren und anderer Interessengruppen rechnen müssen.
Doch die Besorgnis, Opfer von Cyberattacken zu werden, schlägt sich nicht nachhaltig in


© peterschreiber.media/AdobeStock

den Security-Maßnahmen nieder. Dafür gibt es viele deutliche Anzeichen.

Security-Budgets weiterhin zu niedrig, Security-Schulungen zu selten

Trotz steigender Cyberrisiken in Zeiten von Homeoffice und Corona-Pandemie haben viele Unternehmen nicht so auf die Bedrohungslage reagiert, wie man es erwarten sollte. So hat die Wirtschaftsumfrage des BSI

(Bundesamt für Sicherheit in der Informationstechnik) ergeben, dass über 50 Prozent der Unternehmen weniger als zehn Prozent der IT-Ausgaben in Cyber-Sicherheit investieren. Das BSI empfiehlt jedoch, bis 20 Prozent des IT-Budgets in Sicherheit zu investieren. Selbst eher kostengünstige Sicherheitsmaßnahmen wie Notfallübungen oder der Grundsatz „IT-Sicherheit ist Chefsache" werden nicht genügend umgesetzt, so das BSI. „IT-Sicherheit ist noch zu wenig in Budgets, Abläufen und Köpfen der Unternehmen angekommen", erklärt dann auch Arne Schönbohm, Präsident des BSI.

Auch der Digitalverband Bitkom berichtet, dass die Sicherheitsmaßnahmen der Unternehmen nicht der Bedrohungslage entsprechen, obwohl diese durchaus gesehen wird. Im Zuge der Corona-Pandemie hat besonders die Absicherung von Cloud-Anwendungen an Bedeutung gewonnen. Sie sind vielfach notwendig, um Mitarbeitenden die Arbeit aus dem Homeoffice zu ermöglichen.

Allerdings werden passende Sicherheitsmaßnahmen von etlichen Unternehmen im Land nicht genutzt, so Bitkom: 60 Prozent setzen zwar auf abhörsicherer Sprachkommunikation, nur 46 Prozent allerdings auf erweiterte Verfahren zur Benutzeridentifikation – also etwa die Anmeldung auf einem Gerät mittels Zwei-Faktor-Authentifizierung. Gegen den Datenabfluss von innen sichern sich 43 Prozent ab, 42 Prozent separieren Netzwerkzugänge für Kunden oder Geschäftspartner und 41 Prozent verschlüsseln ihren Mailverkehr.

„Viele Sicherheitsmaßnahmen lassen sich mittlerweile leicht umsetzen und mit wenig Vorlaufzeit im Arbeitsalltag integrieren. Trotzdem steigt deren Nutzung nur langsam. Die Zuwächse sind zwar grundsätzlich ein positives Signal, Unternehmen sollten aber keine Zeit verlieren und ihre Sicherheit ausbauen", kommentierte Bitkom-Geschäftsleiterin Dehmel.


© Production Perig/AdobeStock

Auch Nutzer sorgen sich, handeln aber nicht entsprechend

Umfragen zur IT-Sicherheit wie die des Digitalverbands Bitkom machen deutlich, dass es nicht nur auf Unternehmensebene eine Diskrepanz zwischen der Furcht vor den Cybergefahren und dem tatsächlichen Handeln gibt. Auch auf der Ebene der Nutzer kann man dies feststellen:

Auf der einen Seite steht die Erfahrung mit der Internetkriminalität. Acht von zehn Personen (79 Prozent) waren in den vergangenen zwölf Monaten von kriminellen Vorfällen im Netz betroffen. Nur noch eine kleine Minderheit von 21 Prozent gibt an, keine solchen Erfahrungen gemacht zu haben.

Auf der anderen Seite steigt das Vertrauen in die Internetsicherheit. Laut Bitkom erholt sich das Vertrauen in die Datensicherheit im Internet mit jedem Jahr mehr: Drei von zehn

Internetnutzern (29 Prozent) finden, dass ihre persönlichen Daten im Internet sicher sind. Im Jahr 2019 gaben dies 27 Prozent an, 2014 lag der Wert bei gerade einmal 14 Prozent.
Für die Sicherheit der Daten sehen sich Internetnutzer dabei immer stärker selbst verantwortlich. Fast neun von zehn (86 Prozent) sagen: Ich bin selbst für den Schutz meiner persönlichen Daten im Internet verantwortlich. Im Jahr 2019 waren es 78 Prozent und im Jahr 2014 erst 62 Prozent.
Doch fühlen sich aber nur 39 Prozent in der Lage, ihre Geräte wie Smartphone oder Computer selbst vor Angriffen durch Internetkriminelle zu schützen. 63 Prozent sagen, sie würden nicht bemerken, wenn der Computer oder das Smartphone ausspioniert würde. Entsprechend groß ist die Bereitschaft, diese Wissenslücke zu schließen: 56 Prozent würden sich gerne weiterbilden, um sich im Internet besser schützen zu können.
Eine Weiterbildung in Security wäre auch wirklich geboten. Ein Beispiel dafür: Mehr als ein Drittel (35 Prozent) der Smartphone-Nutzerinnen und -Nutzer in Deutschland hat das eigene Gerät mindestens einmal verloren. Weitere neun Prozent haben ihr Smartphone bereits unabsichtlich liegen gelassen und es später wiedergefunden.

Security Awareness ist und bleibt eine Daueraufgabe

Eine Befragung von Bitkom zeigt aber auch: Eine Schulung der Mitarbeitenden zu Sicherheitsthemen nehmen erst 56 Prozent der befragten Betriebe vor. Dazu Bitkom-Expertin Dehmel: „Unvorsichtige oder schlecht geschulte Beschäftigte können schnell zum Ziel von Angriffen werden. Investitionen in Schulungen sind deshalb immer auch wichtige Investitionen in die Zukunft des Unternehmens.

© sitthiphong/AdobeStock

Dabei ist zentral, die Mitarbeitenden gezielt für ihren spezifischen Arbeitskontext weiterzubilden.“
Sicherheitsbehörden betonen entsprechend der Risken durch mangelnde Security Awareness: Nach wie vor eine wichtige Rolle spielt der Faktor „Mensch“ als Einfallstor für Angriffe, so das BSI im aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland. Die Unsicherheit und Überforderung durch die COVID-19-Pandemie, der reale und empfundene Zeitdruck sowie die gesellschaftliche und mediale Dominanz des bestimmenden Themas wurden im Berichtszeitraum von Angreifern ausgenutzt, um Opfer durch Phishing-Angriffe und andere Betrugsformen zur Herausgabe sensibler Informationen oder personenbezogener Daten zu bewegen. Daten-Leaks, Cyberangriffe auf Videokonferenzen, schlecht abgesicherte VPN-Server oder der Einsatz privater IT im beruflichen Kontext führten zu Sicherheitsvorfällen.

Es stellt sich die drängende Frage, wie die Security Awareness auf die Bedrohungslage besser angepasst werden kann.

Security Awareness braucht Individualität und Automatisierung

Betrachtet man die aktuellen Herausforderungen in der Security Awareness, stellt man fest: Wer die Security Awareness im Unternehmen verbessern will, muss für mehr Sicherheit werben. Werbung arbeitet bekanntlich zielgruppenspezifisch. Die Zielpersonen werden in der Werbung abhängig nach ihren Interessen unterschiedlich angesprochen, genauso muss es die Security Awareness tun.

Die Interessen hängen unter anderem davon ab, welche Aufgabe man hat. So beschäftigt sich eine Bereichsleiterin für Finanzen natürlich mit anderen Themen als jemand aus der IT-Abteilung. Entsprechend muss eine erfolgreiche Security Awareness auf das jeweilige Unternehmen und die Zielgruppe der Trainings zugeschnitten sein. Security Awareness „von der Stange" reicht nicht aus, um das Bewusstsein für Security nachhaltig zu steigern.

Eine weitere Herausforderung: An dem Fachkräftemangel in der Security gibt es keinen

© Jörg Habermeier/AdobeStock

Zweifel. Er ist auch einer der Gründe, warum man alle Beschäftigten als Teil der Security ansehen muss. Doch für die Durchführung der Security Awareness Trainings braucht es die richtige Expertise. Abhilfe schaffen kann hier Automatisierung. Sie kann die Security-Abteilung im Unternehmen entlasten und regelmäßige Maßnahmen im Bereich der Security Awareness gewährleisten, die sonst unter dem Fachkräftemangel der Security leiden würde.

Oliver Schonschek

Eckes-Granini verwandelt seine Cybersecurity-Kultur mit Hoxhunt Awareness Training

E-Mail-Bedrohungen sind das vorherrschende Sicherheitsrisiko bei Eckes-Granini. Mit Hilfe des Security Awareness Trainings von Hoxhunt konnte dieses Risiko drastisch reduziert werden.

Das Unternehmen

Die Eckes-Granini Gruppe ist der führende Anbieter von Fruchtsäften und Fruchtgetränken in Europa. Mit Sitz in Nieder-Olm, Rheinhessen in Deutschland ist Eckes-Granini europaweit vertreten. Verbraucher in über 80 Ländern weltweit kennen und schätzen ihre Fruchtsäfte und das breite Angebot an Fruchtgetränken.

Die Herausforderung

E-Mail-Bedrohungen wurden als vorherrschendes Sicherheitsrisiko identifiziert, jedoch wurden bereits existierende Awareness-Trainingsprogramme für Cybersecurity aufgrund ihrer standardisierten und nicht auf individuelle Bedürfnisse zugeschnittenen Inhalte sowie einem Mangel an bedeutsamen Ergebnissen durchweg für nicht zufriedenstellend befunden.

Die Lösung

Eckes-Granini hat sich aufgrund des vollautomatischen Services und der hohen Beteiligungsrate der Nutzer für Hoxhunt entschieden. Hoxhunt ist eine automatisierte Plattform, die das Security Awareness Training mit individuell angepassten Lernwegen, die auf dynamischen und gamifizierten Inhalten basieren, anbietet.

Im Folgenden kommentiert Fritz Worsch, CISO bei der Eckes-Granini Group, den Einsatz und die Erfolge des Hoxhunt Security Awareness Trainings:

Onboarding und Engagement

„Ich arbeite seit 30 Jahren in der IT-Branche und habe noch nie ein derart professionelles Onboarding erlebt, wie Hoxhunt es mit uns durchgeführt hat. Über 70% unserer Mitarbeiter*innen in unserem Unternehmen wurden


© chinnarach/AdobeStock

geonboardet und die meisten davon bleiben engagiert und führen die Trainingssimulationen aus. Dies sind viel mehr als wir jemals hatten und alle meine Erwartungen wurden übertroffen. Das Hoxhunt Onboarding-Programm ist rigide, aber genau so, wie es gemacht werden muss. Im Endeffekt ist es sehr hilfreich, ein gut definiertes Onboarding-Programm zu haben. Ich war sehr glücklich."

Dynamisch und kontinuierlich

„Die drei großen Erkenntnisse meinerseits fingen erstens damit an, dass ich sehen konnte, dass Hoxhunt nicht statisch ist wie die anderen Angebote, die wir ausprobiert haben; Hoxhunt entwickelt sich parallel zu der Landschaft der Bedrohungen. Die zweite Sache ist, dass Hoxhunt nicht einfach nur eine Phishing-E-Mail an jeden sendet, sondern diese kontinuierlich verschickt, damit niemand sie vorausahnen kann. So bekommen Menschen ein ständiges Bewusstsein für Cybersecurity. Der dritte Punkt ist, dass ich es sehr interessant finde, wie dynamisch das Training ist. Wenn jemand eine Phishing-Simulations-E-Mail bekommt und richtig reagiert, wird er oder sie beim nächsten Mal mit einer schwierigeren Simulation herausgefordert. Wenn sie nicht erkannt wird, bekommen sie beim nächsten Mal eine einfachere Simulation. Den Schwierigkeitsgrad zu variieren führt dazu, dass Menschen am Ball bleiben."

Automatisierung

„Automatisierung spart eine Menge an Ressourcen und sie hilft, die Ressourcen richtig zu lenken. Sie hilft, auf Kurs zu bleiben und sicherzugehen, dass wir die richtigen Menschen zur richtigen Zeit ansprechen."

Bedrohungen melden

„Unsere Sicherheitskultur hat sich definitiv verändert. Der Hoxhunt-Button selbst hat sich als zusätzliche Chance erwiesen, alle

Ergebnisse

- Dutzende von gezielten, unterschiedlich simulierten E-Mails werden jährlich an jede/n Angestellte/n gesendet
- Gesteigertes Reporting von echten Bedrohungen über den Hoxhunt-Button
- Globale signifikant verbesserte Security-Kultur
- Vermindertes Risiko von Schädigungen durch E-Mail-Angriffe
- Über 70 % der Mitarbeiter konnten in das Trainingsprogramm eingegliedert werden
- 70 % Beteiligungsrate: Wenn die Angestellten einmal damit anfangen, bleiben sie am Ball

70%+

der Mitarbeiter konnten in das Trainingsprogramm eingegliedert werden

70%

Beteiligungsrate: Wenn die Angestellten einmal damit anfangen, bleiben sie am Ball.

möglichen ankommenden Phishing- und Spam-E-Mails zu lenken und an die richtigen Orte zu verschieben. In der Vergangenheit wussten die Mitarbeiter nicht, wen sie kontaktieren sollten, was dazu führte, dass potentiell schädliche E-Mails ignoriert, zu mir oder zu unserem externen Partner weitergeleitet wurden. Jetzt ist das Melden für unseren Endbenutzer leicht, wir pushen sie, den Button zu verwenden und sagen ihnen, dass dies der einzige Weg ist, uns zu informieren, dass sie eine verdächtige E-Mail erhalten haben."

Fazit

„Ich würde Hoxhunt definitiv anderen CISOs weiterempfehlen und habe dies auch bereits getan. Hoxhunt geht weit über die traditionelle Häkchen-Mentalität des passiven E-Learnings hinaus. Unsere Security-Kultur hat sich definitiv verändert seit wir angefangen haben, Hoxhunt zu nutzen. Hoxhunts gamifizierte Trainingsplattform holt die Mitarbeiter*innen

© NicoElNino/AdobeStock

auf ihren individuellen Fähigkeitslevels automatisch ab und trainiert sie darauf, verdächtige E-Mails zu melden. Im Ergebnis nehmen wir weitaus mehr Meldungen von echten Bedrohungen wahr. Und das Customer Success Team von Hoxhunt ist erste Klasse. Sie haben uns zu einer Onboarding-Rate der Angestellten von 70% weltweit in unserem Unternehmen verholfen. Ich arbeite seit 30 Jahren in der IT-Branche und habe noch nie ein derart professionelles Onboarding erlebt wie bei Hoxhunt."

Powered by:

HOXHUNT

Hoxhunt
Porkkalankatu 3
00180 Helsinki, Finland
Telefon +358 20 530 2100
Web www.hoxhunt.com

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21
86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel.de
Erscheinungstermin: April 2022
Titelbild: NicoElNino/stock.adobe.com

VOGEL IT MEDIEN