Vorstand Gerd Hundertmark (rechts) freut sich zurecht mit seinem Team der Wohnungsgenossenschaft Hameln über das blütenweiße Ergebnis bei der „Social Hacking Übung". Keine Phishing-Mail wurde geöffnet. Vorbildlich. Dafür löste der Chef sein Versprechen ein: Pizza für alle!

Überregionaler Erfahrungsaustausch „Social Hacking Übung für Firmen"

VON VOLKER KOHLHARDT, TRAINSTITUTE®

Berlin. Als Kooperationspartner der wohnungswirtschaftlichen Regionalverbände aus Baden-Württemberg (vbw), Bayern (VdW Bayern), Niedersachsen/Bremen (vdw), Norddeutschland (VNW) und Thüringen (vtw) hat Trainstitute® einen Erfahrungsaustausch als Online-Meeting organisiert.

Trainstitute® führt Social Hacking Übungen durch, die einerseits – ähnlich einer Brandschutz-Übung – das Risikobewusstsein der Belegschaft trainieren und zeitgleich einen Status über das tatsächliche Risikoverhalten der Mitarbeitenden im Arbeitsalltag abbilden. Über 50 wohnungswirtschaftliche Unternehmen haben eine solche Social Hacking Übung mit Trainstitute® in diesem Jahr durchgeführt. Auf Wunsch der teilnehmenden Wohnungsunternehmen gab es kürzlich einen Erfahrungsaustausch zum Thema und den Übungsergebnissen.

Volker Kohlhardt von Trainstitute® begann mit einem kurzen Überblick über die Ergebnisse (Klickraten) der Gruppen-Kampagne. Während die absoluten Zahlen den „aktuellen Risiko-Reifegrad" der Unternehmung widerspiegeln, hilft die Gegenüberstellung mit vergleichbaren Unternehmen der gleichen Branche, das Ergebnis besser zu verorten.

Die Übung umfasste vier E-Mails, die innerhalb eines Monats gesendet wurden. Gemessen wurden die „Klickraten", sprich: der Anteil der angeklickten Mails oder Links bzw. der Dateneingaben, welche von den Testmails ausgingen. Insgesamt lag die durchschnittliche Klickrate bei 9,8 Prozent. Die Klickraten je Firma reichten von 0 Prozent bis 26,5 Prozent. Auf Ebene einzelner E-Mails zeigten sich Quoten von bis zu 60 Prozent je Firma. Es ist drei Unternehmen gelungen, die Phishing Übung mit 0 Prozent Klickrate zu absolvieren.

Wenn man sich vergegenwärtigt, dass bei einer Phishing Attacke schon eine einzelne Person durch ihr sorgloses Verhalten bzw. durch Unwissen großen Schaden verursachen kann, dann können Klickraten von durchschnittlich fast 10 Prozent als Ausdruck einer relevanten Gefährdung angesehen werden. Eine Unterscheidung in zwei Größenklassen (0-20 Mitarbeitende, über 21 Mitarbeitende) ergab keine signifikanten Ergebnis-Unterschiede.

Ziel und Anlass dieses Online-Meeting war es, gute und weniger gute Erfahrungen, aber auch mögliche Lösungsalternativen zu diskutieren. Folgende Aspekte wurden im Plenum diskutiert:

1. **Auswahl des EDV-Dienstleisters** (soweit dies outgescourced ist)
2. **Cyber-Versicherung**
   (Leistungsumfang, Relevanz und prozessuale Konsequenzen)
3. **Benutzer-Konzept**
4. **Namentliche Nennung von Mitarbeitenden auf Homepage**
5. **Incentivierung**
6. **Wichtigkeit des Themas/Schulungskonzept**

1. Auswahl des EDV-Dienstleisters

Wohnungswirtschaftliche Unternehmen haben nicht selten die EDV-Administration an einen darauf spezialisierten Dienstleister übergeben. Im Rahmen der Social Hacking Übung werden im Vorfeld – dem sogenannten Quality Gate – einige Einstellungen an den Spam-Filtern vorgenommen. Damit wird sichergestellt, dass die E-Mails wirklich beim Mitarbeiter und nicht im SPAM-Ordner landen. Kohlhardt berichtete, dass in einigen, wenigen Fällen die Phishing Übung nicht durchgeführt werden konnte, weil die (externen) EDV-Dienstleister nicht in der Lage waren, die notwendigen Einstellungen („Whitelisting von sicheren Domains und IP-Adressen" nur für die Übung) zu konfigurieren. Thomas Froese (EDV-Leiter vbw) berichtete von ähnlichen Fällen. Auch wenn es bei einer Social Hacking Übung ausschließlich um den Faktor „Mensch" als Teil der Sicherungskette geht, so steht und fällt die EDV-Sicherheitsinfrastruktur mit der Qualität des EDV-Dienstleisters. Eine Möglichkeit, dies zu überprüfen, könnte sein, einen sogenannten Penetrationstest durchzuführen – am besten von einer anderen Firma als diejenige, die die EDV-Betreuung verantwortet.

2. Cyber-Versicherung

Froese berichtete von seinen Erfahrungen mit einer Cyber-Versicherung. In der Diskussion stand weniger die „finanzielle Versicherungsleistung" als vielmehr der Leistungsaspekt „EDV-Forensik". Dieser umfasst die Untersuchung, ob und wenn ja, in welchem Umfang die EDV-Systeme kompromittiert wurden. Das Leistungsspektrum solcher Versicherungen reicht mittlerweile bis zur professionellen PR-Betreuung, wenn ein Erpressungsfall eingetreten ist. Die Diskussion zeigte, dass Cyber-Versicherungen als eine sinnvolle Ergänzung angesehen werden. Denn auch eine sehr gut funktionierende EDV-Sicherheitsinfrastruktur und gut geschulte, aufmerksame Mitarbeitende können das Rest-Risiko nicht ausschließen.

3. Benutzer-Konzept

Hier wurden zwei ganz simple und zugleich sehr wirksame Methoden diskutiert. VNW-Verwaltungsleiter Andreas Thal wies darauf hin, dass insbesondere bei Geschäftsleitungen darauf geachtet werden sollte, dass diese wirklich nur solche Zugriffsrechte erhalten, die sie operativ benötigen. Geschäftsleitungsmitglieder stehen ohnehin im Fokus, denn sie sind häufig auf den Webseiten namentlich und mit E-Mail-Adresse aufgeführt und daher leicht zu identifizieren und zu kontaktieren. Und wenn sie dann „qua Position" im Benutzerkonzept für alles freigeschaltet werden, dann ist im Angriffsfall der Schaden groß. Thomas Froese beschrieb noch eine zusätzliche Möglichkeit, hier Schaden von der Unternehmung fernzuhalten: Sollte die Geschäftsleitung operativ umfangreiche Rechte benötigen, so könnte für weitergehende, potenziell kritische Vorgänge eine weitere, öffentlich unbekannte E-Mail-Adresse für ein Mitglied der Geschäftsführung verwendet werden (Beispiel E-Mail Tagesgeschäft: name@firma.de und für sensible Anwendungen name-admin@firma.de).

4. Incentivierung

Die Ergebnisse der Social Hacking Übung haben auch gezeigt, dass es Unternehmen gibt, deren Belegschaften augenscheinlich sehr besonnen auf die Phishing Mails reagiert haben. Hier war natürlich von großem Interesse zu erfahren, was diese Firmen dafür getan haben. Trainstitute® empfiehlt grundsätzlich immer, die Übung in der Belegschaft vorher anzukündigen. Dafür gibt es zwei Gründe:

1. Die Ankündigung erhöht die Aufmerksamkeit von Anfang an – und Aufmerksamkeit ist ja das eigentliche Ziel. Anders ausgedrückt: Die Ankündigung schadet nicht! Außerdem kann bei der Ankündigung auch gleich ein Hinweis gegeben werden, wie die Kollegen sich verhalten sollen. Konkret: Wie sollen sie mit der Nachricht umgehen? Wen sollen sie kontaktieren, wenn sie eine fragwürdige E-Mail erhalten? Diese Verhaltensanweisung gilt ja über die Übung hinaus und ganz generell.
2. Wenn eine solche Übung nicht angekündigt wird, kann es auf Seiten der Belegschaft Fragen aufwerfen wie zum Beispiel „Will mich mein Arbeitgeber kontrollieren? Traut man mir nicht?". Dies kann zu „atmosphärischen Verstimmungen" führen.

Gerd Hundertmark, Vorstand der Wohnungsgenossenschaft Hameln, berichtete, dass er die Übung angekündigt hat – und eine Belohnung in Form einer „Pizza" ausgerufen hat, wenn es der Belegschaft gelingt, mit 0 Prozent Klickrate die Übung zu absolvieren. Gleichzeitig kündigte er an, dass die Social Hacking Übung im Laufe der nächsten sechs Monate wiederholt wird, dann jedoch ohne gesonderte Ankündigung. Diese Variante bewahrt alle Vorteile des offenen Umgangs und hält das hohe Maß an Aufmerksamkeit über Monate hinweg aufrecht. Dieses Vorgehen als „gemeinsame Herausforderung" zu deklarieren und mit einer Belohnung zu kombinieren, folgt den Erkenntnissen von „Gamification".

Fazit übrigens: Die WGH hat tatsächlich das große Ziel erreicht. Gerd Hundertmark ließ sich nicht lumpen und spendierte die versprochene Pizza.

5. Wichtigkeit des Themas / Schulungskonzept

Kohlhardt führte aus, dass seiner Erfahrung nach drei Komponenten nötig sind, um in Firmen das Thema EDV-Sicherheit in Bezug auf die Mitarbeiter-Sensibilisierung erfolgreich umzusetzen:

1. Die Unternehmensleitung muss dem Thema für die Belegschaft erkennbar einen hohen Stellenwert beimessen.
2. Es braucht systematische Schulungskonzepte, die alle Mitarbeitenden erreicht, ihren individuellen Vorkenntnissen und Lernpräferenzen gerecht wird und in einem arbeitsalltagstauglichen Format durchgeführt werden. Ein solches Schulungskonzept beinhaltet auch dokumentierte Wissensstandsüberprüfungen. Die von Trainstitute® ebenfalls angebotenen Video-Schulungen erfüllen diese Anforderung.
   (Bsp: www.vdw-online.trainstitute.de/)
3. Neben der Vorbild-Funktion durch die Unternehmensleitung und der Wissensvermittlung bzw. dem Verständnisaufbau ist der Aspekt „praktisches Üben" (wie zum Beispiel durch eine regelmäßig zu wiederholende Social Hacking Übung) hilfreich, theoretisches Wissen in alltägliches Bewusstsein und Handeln zu überführen.

Weitere Erfahrungsaustausche sind geplant. Die Teilnahme ist kostenlos und steht allen Mitgliedsunternehmen offen. Bei Interesse einer Teilnahme wenden Sie sich gern an Volker Kohlhardt (kohlhardt@trainstitute.com).