hatte. Die Herausforderung auf der blauen Seite bestand darin, diese Einfallstore zu finden und den Zugriff zumindest einzuschränken.

Ein spezielles Cisco-Team wurde seitens der Roten eingesetzt, um die Router anzugreifen. Dabei ging es vor allem darum, Passwörter und Nutzernamen zu kompromittieren und die Konfiguration der einzelnen Systeme herauszufinden. Einen ähnlichen Ansatz verfolgte ein spezielles Ericsson-Team, das Angriffe auf die Mobilfunksysteme ausführte.

Die zweitägige aktive Übungsphase stellte sich als Härtetest für alle Übungsteilnehmer heraus, der der Kreativität der Angreifer wie der Verteidiger alles abverlangte. So ging im Minutentakt die Kontrolle einzelner Systeme verloren oder wurde wiedergewonnen. Dabei mussten die Blauen ständig Kompromisse eingehen, um beispielsweise die Nutzbarkeit der einzelnen Systeme nicht durch zu starke Härtungsmaßnahmen einzuschränken. Am Ende blieb aber nichts anderes übrig, als einzelne Teilbereiche aufzugeben, um die wirklich wichtigen Komponenten im komplexen Netzwerk abzusichern.

Ziel der Veranstalter war es, durch ständig erhöhte Angriffsintensität Stresssituationen zu erzeugen. Diese sollten strategische Entscheidungen erzwingen oder auch Fehlentscheidungen provozieren.

Am Ende gelang es dem deutschen Blue Team, die Schlüsselpositionen zu halten und mithilfe des ungarischen Teams die Strom- und Wasserversorgung zu sichern. Unter diesen extremen Bedingungen konnte ein sehr guter achter Platz erreicht werden. Das deutsche Forensik-Team leistete zu diesem Erfolg einen besonderen Beitrag, indem es zum vierten Mal in Folge in dieser Wertung den ersten Platz belegte.

Letztendlich errang das französische Blue Team den ersten Platz, dicht gefolgt von der Tschechischen Republik und Schweden.

Die beteiligten Teams

Blau: Die Verteidiger

30- bis 50-köpfige Teams, die von ihren Standorten aus agieren und per VPN mit dem Übungsnetz verbunden sind.

Rot: Die Angreifer

IT-Sicherheitsexperten, die auf Angriffe auf Computernetzwerke spezialisiert sind. Sie treten in kleineren Gruppen auf und konzentrieren sich auf die Bereiche Clients, Server, Webapplikationen oder Firewall und Router. Sie agieren von Tallinn aus.

Gelb: Die Nutzer

Sie bedienen die Informationstechnik im Einsatzland. Sie simulieren die Beschäftigten in Firmen und Kraftwerken und führen bestimmte Aktionen aus, die in Drehbüchern festgelegt sind – das bedeutet, sie handeln, wie es normale Nutzer auch tun würden. Hier waren vorrangig Studenten der Technischen Universität Tallinn eingesetzt.

Weiß: Die Schiedsrichter

Das Team wertet das automatisierte Punktesystem aus und greift bei strittigen Situationen korrigierend ein. Hier sind auch die simulierten Pressevertreter angesiedelt, die Informationen mit den Blue Teams austauschen dessen Reaktionen bewerten.

Grün: Die Techniker

Sie sind für das Übungsnetzwerk und alle virtuellen Systeme verantwortlich. Dies umfasst auch die VPN-Verbindung zu den Standorten der verschiedenen Blue Teams.

Fazit

Bei den Locked Shields handelt es sich um die weltweit größte Live Fire Cyber Defence Exercise, die im Vergleich zu den Vorjahren noch einmal einen höheren fachlichen Anspruch hatte. Der eigentliche Sinn der Übung besteht sicherlich nicht im Sammeln von Punkten. Sie trainiert aber alle Beteiligten auf einem sehr hohen technischen Niveau auf realen Systemen. Dabei umfasst die Übung alle Facetten einer möglichen Auseinandersetzung im Cyberraum.

Im Vergleich insgesamt lagen die Nationen im vorderen Bereich, die diese Übung als Schwerpunkt ihrer Tätigkeit sehen und über das gesamte Jahr trainieren. In diesem Zusammenhang ist es besonders wichtig, sowohl eine gute Mischung von Systemadministratoren und IT-Sicherheitsfachleuten als auch von jüngerem und erfahrenem Personal zu erreichen. Daher arbeiten einige Blue Teams mit externen Organisationen und Firmen zusammen, die bereits über notwendige Fähigkeiten verfügen.

Insgesamt hat sich gezeigt, dass militärische Organisationen, zivile Behörden und Institutionen zusammenarbeiten können, um bei möglichen Auseinandersetzungen im Cyberraum erfolgreich zu agieren. (ur@ix.de)

Quellen

Hintergrundinformationen zu den Organisatoren und Teilnehmern der Locked Shields, Fotos der Veranstaltung sowie das Handbuch zu Cobalt Strike Beacon sind über ix.de/z5kq zu finden.

Das Angriffs-Framework Cobalt Strike

Cobalt Strike ist ein von Raphael Mudge geschriebenes kommerzielles Framework, das vorrangig von Penetrationstestern und Red Teams eingesetzt wird. Es verfügt über Werkzeuge, die helfen Informationen zu beschaffen, Schwachstellen zu finden, in IT-Systeme einzudringen und sich im Netzwerk festzusetzen. Dabei werden Techniken angewendet, die auch reale Gegner einsetzen, wenn sie keine oder nur geringe Informationen über ein Zielsystem haben.

Mit dieser Java-Applikation lassen sich Phishingangriffe ausführen und Software on the fly mit Malware infizieren. Die Angreifer stehen dabei untereinander in Verbindung und sind in der Lage, relevante Informationen auszutauschen.

Ein sogenannter Beacon ist eine Payload in Cobalt Strike, die die Kommunikation mit einem kompromittierten Host über einen langen Zeitraum gewährleistet. Dabei ist es irrelevant, ob die Payload über einen Clientangriff gesendet oder in eine bereits bestehende Session injiziert wurde. Einmal im Zielsystem integriert, kann sie zeitgesteuerte Aufgaben ausführen oder Informationen weitergeben.

Dipl.-Ing. (FH) Frank Neugebauer

hat als Offizier der Bundeswehr über 25 Jahre auf dem Gebiet der IT-Sicherheit gearbeitet. Seit 2017 ist er im Ruhestand und noch immer als Berater und externer Mitarbeiter tätig. Er ist außerdem Autor des Buches „Penetration Testing mit Metasploit".

Awareness-Projekt der Landeshauptstadt Kiel

Schlaue Fische

Werner Degenhardt, Andreas Amann, Frank Weidemann, Jan Koppelmann

E-Mails und besonders Phishingmails sind noch immer der Angriffsvektor Nummer eins in Unternehmen. Die Schwachstelle ist wie so oft der Mensch.

Schon im Jahr 2000 stellte der Sicherheitsexperte Bruce Schneier fest, dass sich die IT-Welt nach der Ausbeutung von Schwächen in Hardware und Software schon mitten in der dritten „semantischen" Welle von Netzwerkangriffen befinde: die Angriffe auf Menschen, die Hardware und Software benutzen. Diese seien schlimmer als physische oder syntaktische Angriffe, denn, so Schneier, sie „richten sich direkt auf die Mensch-Maschine-Schnittstelle, die unsicherste Schnittstelle im Internet. […] Und jeder Versuch zur Lösung des Problems muss sich mit Menschen auseinandersetzen, nicht mit der Technik."

Am besten begriffen hat das die Phishing-Branche, die mit immer ausgefeilteren Angriffsplänen Personen in Unternehmen, in der öffentlichen Verwaltung und in Privathaushalten zu Handlungen veranlasst, die alle technischen Bemühungen um Informationssicherheit und Datenschutz aushebeln.

Sensibilisierung liegt im Argen

Seit 20 Jahren versuchen Sicherheitsexperten, die „Human Firewall" zu stärken und Benutzer zu besserem Sicherheitsverhalten zu erziehen. Das Mittel der Wahl sind sogenannte Awareness- oder Sensibilisierungskampagnen, die im Wesentlichen dem von der europäischen Sicherheitsbehörde ENISA vorgeschlagenen Schema folgen (Abbildung 1).

Sensibilisierungskampagnen hatten und haben große Ähnlichkeit mit der Werbung für Produkte in einem Käufermarkt. Bei der Änderung von Sicherheitsverhalten geht es aber um Verhalten in einem komplexen Kontext und nicht um die Entscheidung, ein Produkt zu kaufen. Das ist ein großer Unterschied.

Das ENISA-Schema zeigt ganz richtig, dass der Weg vom Kontakt mit einem Problem bis zur dauerhaften Änderung des Verhaltens, das zu diesem Problem führt, ein langer Weg bergauf ist. Kritisch ist vor allem, dass alles, was nach der „Sensibilisierung" kommt, irgendwie von selbst geschehen soll und dem Willen des Benutzers zur Selbstverbesserung überlassen bleibt.

Dass das so einfach nicht funktioniert, weiß jeder, der sich zum neuen Jahr einige Verhaltensänderungen (mehr Sport, weniger und gesünder essen et cetera) vorgenommen hat. Die eigene Erfahrung mit den Neujahrsvorsätzen zeigt, was die Gesundheits- und Umweltpsychologie an vielen Beispielen eindrucksvoll belegt hat: Es ist schwer, Gewohnheiten zu ändern. Mit Informationskampagnen und Appellen an die Verantwortung für sich selbst oder andere hat man in den seltensten Fällen Erfolg. Das liegt vor allem an zwei Eigenschaften der menschlichen Natur. Erstens: Der Weg vom Wissen zum Handeln ist weit. Zweitens: Der Mensch mag keine Änderungen.

Der Weg vom Wissen zum Handeln ist weit

Sensibilisierungsprofis sind in den letzten 20 Jahren dem Irrtum erlegen, dass man die Human Firewall durch Vermittlung von Wissen härten kann. Die Vorstellung war und ist es auch vielfach noch, dass man nur erklären muss, wie gefährlich zum Beispiel eine E-Mail sein kann, und schon verhalten sich die Belehrten vorsichtig und richtig. Das funktioniert so aber nicht, wie wissenschaftliche Untersuchungen zur „Theorie des geplanten Handelns" schon in den Achtzigerjahren herausfanden (Abbildung 2).

Zum Beispiel hört Heiner Müller einen Vortrag über den Angriffsvektor „E-Mail" und weiß danach im Prinzip, dass bei E-Mails – anders als er vorher dachte – nicht alles so ist, wie es scheint und wie

er es sich wünscht. Er hat verstanden, dass E-Mail keine synchrone Kommunikation wie beim Telefon ist, sondern besser mit einer Postkarte zu vergleichen. Da ist auch nichts sicher. Nicht der Absender, nicht die Unversehrtheit auf dem Postweg und es gibt keine Garantie, dass sie überhaupt ankommt (Wissen).

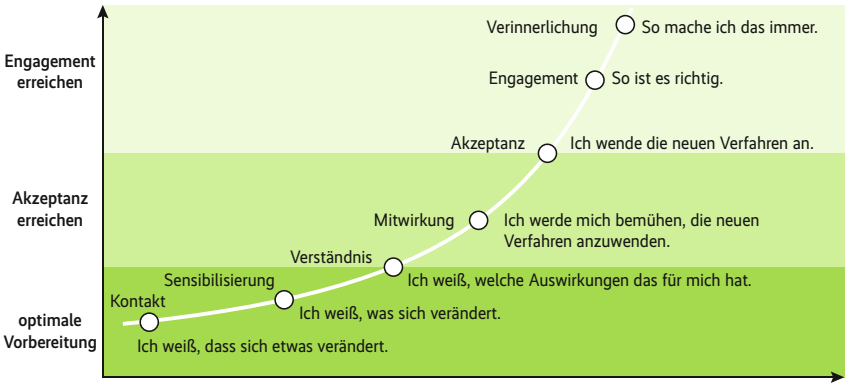
Er hat verstanden und akzeptiert, dass die IT-Abteilung seines Arbeitgebers ihren Mitarbeitern keine vollkommen sichere Arbeitsumgebung zur Verfügung stellen kann und er selbst dazu beitragen muss, dass nichts passiert (Einstellungen).

Er beschließt, sein Wissen im Umgang mit E-Mails einzusetzen (Verhaltensabsicht) und Absender, eingebettete Links und Attachments kritisch zu überprüfen. Vertrauliche Informationen, auch das weiß er, sollte man niemals an Adressen außerhalb des Unternehmens geben. Heiner Müller hat sogar versucht, mithilfe des E-Learning-System seines Unternehmens anzueignen, wie man sich den E-Mail-Header anzeigen lassen und was man daraus alles schließen kann (Fähigkeiten/Fertigkeiten).

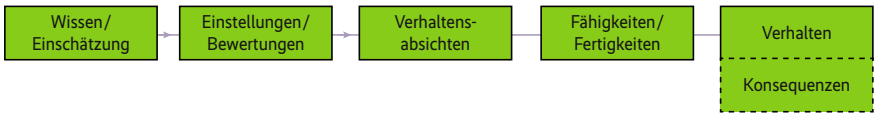
An diesem einen bestimmten Tag ist extrem viel zu tun, E-Mails kommen rein, E-Mails gehen raus. Der Chef schaut kurz vorbei, um etwas Trost und Lob zu spenden. Heiner Müller freut sich, dass er berichten kann: „Ich habe das Geld schon angewiesen. Der Vorgang ist in trockenen Tüchern." Da meint der Chef: „Welche Überweisung? Welcher Vorgang? Ich weiß von nichts." Autsch. Phishingmail. CEO Fraud. Dumm gelaufen (Verhalten/Konsequenzen).

Gewohnheiten sind schwer zu ändern

Bei der Erklärung von Verhalten verwenden die meisten Psychologen heute ein „Dual-Process"-Modell des Denkens, wobei die beiden Prozesse häufig als „System 1" und „System 2" bezeichnet werden.



Wirkungsverlauf von Awareness-Kampagnen: Nur Schritt für Schritt kann man eine nachhaltige Verhaltensänderung herbeiführen (Abb. 1).



In der Theorie zieht man aus dem Gelernten beim nächsten Handeln die Konsequenz – praktisch ist es nicht so einfach, eingefahrene Gewohnheiten und Verhaltensweisen loszulassen (Abb. 2).

System 1 (automatische Verarbeitung) ist schnell, intuitiv, assoziativ, benutzt Instinkte, Heuristiken, Gewohnheiten, Metaphern und Denkgewohnheiten, reagiert auf Umweltreize und kann nicht abgeschaltet werden. Es bewirkt, dass die allermeisten alltäglichen Verhaltensweisen automatisch ablaufen können. Das ist gut so, weil wir sonst an der Komplexität der Welt scheitern würden.

System 2 (systematische Verarbeitung) ist das, was man im Allgemeinen als Ratio oder Bewusstsein bezeichnet. Das bewusste Denken ist langsam, anstrengend und verbraucht die knappe Ressource Aufmerksamkeit. Es ist träge und ermüdet schnell. Es verlässt sich auf die Arbeit von System 1 und springt – ziemlich unwillig – erst dann an, wenn die Dinge schwierig werden.

Der Mensch neigt von Natur aus dazu, Gewohnheiten auszubilden. Er tendiert dazu, ein Verhalten, das sich in einem bestimmten Kontext bewährt hat, immer wieder zu zeigen. Gewohnheiten sind gelernte Reaktionen, die von bestimmten Kontextmerkmalen aktiviert werden. Sie entwickeln sich langsam und verlieren über die Zeit die Bindung an das ursprüngliche Handlungsziel. Gewohnheiten sind extrem resistent gegenüber Belehrungen.

Am ehesten kann man Gewohnheiten ändern, wenn es gelingt, die Handlungskette zu unterbrechen und sofort eine geeignete und akzeptable Alternative anzubieten, und das immer wieder, bis eine neue, bessere Gewohnheit entstanden ist. Eine andere Möglichkeit der Intervention ist die Änderung der Umgebung, deren Merkmale und Anreize die gewohnheitsmäßige Handlungskette auslöst. Das Ändern von Gewohnheiten fällt leichter, wenn man umzieht, eine neue Arbeit anfängt oder das Betriebssystem des Rechners wechselt.

Internet und Informationsgewohnheiten

Viele Verhaltensweisen in IT-Umgebungen, die von Systembetreuern, Informationssicherheitsbeauftragten und Datenschützern der Trägheit oder Dummheit der Benutzerpersönlichkeit zugeschrieben werden, sind nichts anderes als Gewohnheiten, die sich aus gutem Grund so entwickelt haben, wie sie sind.

E-Mail wird oft als die „Killer-Anwendung des Internets" bezeichnet. Sie ist grundlegend in das Kommunikationsgeschehen eingebettet und wird dabei hoffnungslos überbeansprucht durch den Ein-

iX-TRACT

- Nach wie vor sind (Phishing-)E-Mails das häufigste Mittel, Unternehmen Malware unterzuschieben oder an vertrauliche Daten zu gelangen. Sensibilisierung vor allem in diesem Bereich tut not.
- Verhaltensänderungen sind nicht allein auf der Basis von Schulungen durch Zuhören oder Lesen zu bewerkstelligen. Erkenntnisse der neueren Lern- und Verhaltensforschung können hier wertvolle Unterstützung leisten.
- Gelungene Schulungsmaßnahmen können bei Mitarbeitern zumindest ein nützliches Misstrauen erwecken – von dem sie auch im privaten Bereich profitieren.

Informationssicherheit ist schwer zu lernen

In einer üblichen Lernsituation wird Verhalten durch positive Verstärkung geformt. Wenn man etwas richtig macht, wird man belohnt. Bei Sicherheitsentscheidungen besteht die positive Verstärkung darin, dass die Wahrscheinlichkeit, dass etwas Schlimmes geschieht, weniger groß ist. Die Belohnung für sicheres Verhalten ist, dass nichts Schlimmes passiert. Die Entscheidung für Sicherheit hat kein sichtbares Ergebnis und es gibt keine sichtbare Bedrohung.

Wenn aber etwas Schlimmes geschieht – was selten der Fall ist oder nicht bemerkt wird –, kann das Tage, Wochen oder Monate von der falschen Entscheidung entfernt sein. Das macht das Lernen negativer Konsequenzen extrem schwer, ausgenommen im Fall spektakulärer Katastrophen.

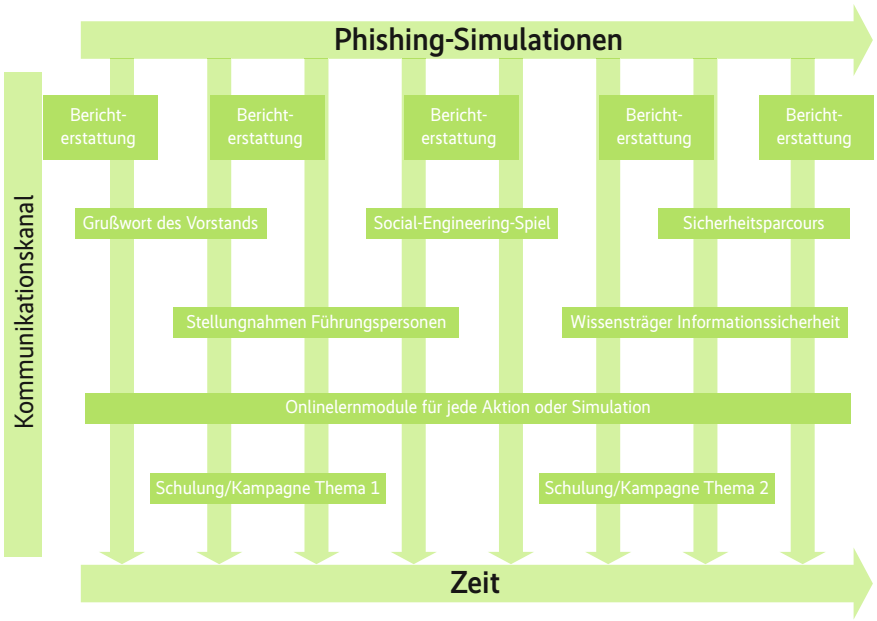
Hinzu kommt, dass die oft benutzten Vergleiche der (digitalen) Informationssicherheit mit der Sicherheit in der analogen Welt einfach nicht passen. Bei der Fahrzeugsicherheit zum Beispiel kann der Fahrer ein Warnschild betrachten und weiß so, dass es in der Nähe eine Schule oder etwas anderes gibt, das Vorsicht erfordert. Das kann man kaum mit dem Klicken auf einen schädlichen Link vergleichen.

Um schädliche Links zu erkennen, muss man etwas über die zugrunde liegende Technik wissen. Es gibt einen großen Unterschied zwischen „Fahren Sie nicht mit dem Auto auf dem Eis“ und „Klicken Sie nicht auf einen schädlichen Link“.

Jeder weiß, was Eis ist. Aber was ist ein „verdächtiger“ Link oder eine verdächtige E-Mail? Um das zu beurteilen, muss der Benutzer die zugrunde liegenden Merkmale betrachten und eine Entscheidung fällen. Er muss den Mauszeiger über den Link bewegen, die URL auf x, y oder z überprüfen und verstehen, was sich dahinter verbirgt. Das wird in der Regel aus Mangel an Zeit und Wissen nicht geschehen. Aus der Not geborene allgemeine Ratschläge der Hüter der Informationssicherheit wie „Gesatz für das Telefonieren mit der Tastatur, das Austauschen und Verwalten von Dokumenten, Aufgaben, Terminen, Adressen und vieles andere, für das E-Mail niemals gedacht war.

Benutzer stellen sich unter E-Mail keine Postkarte mehr vor, sondern sehen ein Werkzeug des persönlichen Informationsmanagements (PIM), das für die Koordination mit anderen Personen in der Organisation und im Privatleben benutzt wird. E-Mail ist heute für ihre Benutzer mehr ein Lebensraum für die Informationsarbeit und -zusammenarbeit als ein einfaches Werkzeug zum Versenden von Nachrichten.

Jeder Benutzer hat es in den vielen Jahren des Ausprobierens und Übens zu einer ausreichend guten Beherrschung seines E-Mail-Clients und zu einer praktikablen Vorstellung seiner Funktionsweise gebracht und nutzt ihn – in seiner ganz individuellen Weise – gewohnheitsmäßig und mit Erfolg.



Das Schulungskonzept zur Härtung der „Human Firewall“ gegen Phishingangriffe basiert auf den neuesten wissenschaftlichen Erkenntnissen des Lernens (Abb. 3).

Effektiv versus vorsichtig

Gewohnheitsmäßig heißt vor allem auch effektiv. Effektives E-Mail-Verhalten bedeutet zum Beispiel bei einer E-Mail von Landeshauptstadt Kiel <info@gehaltskasse.com>, den Absender nur bis zur ersten spitzen Klammer zu lesen und den Friendly Name „Landeshauptstadt Kiel“ als Merkmal für die Vertrauenswürdigkeit des Absenders sowie der ganzen E-Mail zu nehmen, mit allem, was darin enthalten ist.

Auch wenn es eine Phishingmail ist, die wie in diesem Beispiel zum Abfließen persönlicher und schutzwürdiger Daten führt, gibt es keinen Anreiz, die E-Mail-Gewohnheiten zu ändern. Es passiert ja nichts. Zumindest nicht in der Wahrnehmung des Benutzers (siehe Kasten: „Informationssicherheit ist schwer zu lernen“).

Obwohl Informations- und Sensibilisierungskampagnen in den letzten 20 Jahren nicht wesentlich zur Änderung des Nutzerverhaltens geführt haben, stellt sich die Literatur im Bereich der Informationssicherheit das Lernen neuer und besserer Verhaltensweisen immer noch als bewussten Prozess vor und Handlungen als vernunftgesteuert.

Im Wesentlichen plagen die Sicherheitspädagogik die sogenannte Nürnberger-Trichter-Methode (bei der Informationen oben in den Kopf hineingeschüttet werden) und ihre zentralen Annahmen, unter anderem

- der Lehrende weiß, was der Lernende wissen muss;
- Wissen lässt sich mithilfe sprachlicher Darstellungen und Präsentationen vermitteln;
- die Aufgabe des Lernenden besteht darin, sich das Wissen durch Abspeichern im Gedächtnis anzueignen;
- der Lernprozess ist umso erfolgreicher, je mehr Lernstoff vermittelt wird.

Das Ergebnis dieser Methode ist das aus dem Schulunterricht bekannte „träge Wissen“.

Informationssicherheit lernen – Schulungskonzept

Die Theorien und Ergebnisse der Kognitionspsychologie legen nahe, dass erfolgreiches Lernen und vor allem die Neustrukturierung ungünstiger Verhaltensweisen und Gewohnheiten anders erfolgen sollte.

Nach dem Paradigma der konstruktivistischen Didaktik ist Lernen ein längerer Prozess, der die vorhandenen Wissens- und Verhaltensmuster des Lernenden zum Ausgang nimmt und durch situierte Lernumgebungen, Anleitung, Übung und Wiederholung den Lernenden zu besseren Denkstrukturen und besserem Verhalten veranlasst.

Um das Erkennen von Spear-Phishing zu verbessern, muss der Betreffende Spear-Phishing kennenlernen, sich aktiv damit auseinandersetzen und üben, üben, üben.

Eine geeignete situierte Lernumgebung sind Simulationen, in denen der Betreffende mit einer realistischen Phishing-E-Mail angegriffen wird – allerdings ohne ihm wirklich Schaden zuzufügen. Die durch den Angriff erzeugte Betroffenheit – es ist ja wirklich und spürbar etwas passiert – und die dadurch hervorgerufene Aufmerksamkeit für das Thema wird dazu genutzt, ihm zu zeigen, was er beim nächsten Mal besser machen und wo er mehr über das Schema des Angriffs und die Gründe für sein ungünstiges Verhalten erfahren kann.

Das Projekt „Sicherheit für Kommunen in Schleswig-Holstein“ (SiKoSH, siehe Kasten) hat die oben skizzierten Theorien und Ergebnisse der neueren Kognitions- und Lernpsychologie in einem Schulungskonzept zusammengefasst (Abbildung 3).

Live-Phishing-Training bei der Landeshauptstadt Kiel

Die Landeshauptstadt Kiel ist Mitglied im Arbeitskreis SiKoSH und wollte das SiKoSH-Konzept „Sensibilisierung und Schulung“ einem Praxistest unterziehen. Phishing-Simulationen sind in letzter Zeit einfacher geworden, da die Publikumspresse die Themen Informationssicherheit und Datenschutz dauerhaft prominent behandelt und eine ausreichende Grundaufmerksamkeit der Zielpersonen vorausgesetzt werden kann.

Im Fall der Landeshauptstadt Kiel kommt hinzu, dass die vier für den Erfolg der Maßnahme kritischen Rollen das Vorgehen unisono befürworteten: der Oberbürgermeister (Leitung), die Mitarbeitervertretung (Personalrat), ein Datenschutzbeauftragter sowie die IT-Abteilung.

Der in der Phishing-Simulation verwendete „co3tools Phishing Simulator“ basiert auf einer Open-Source-Anwendung und soll nach entsprechender Anpassung allen interessierten Anwendern unter bestimmten Bedingungen zur Verfügung gestellt werden.

Das Live-Phishing-Training für die Mitarbeiterinnen und Mitarbeiter der Landeshauptstadt Kiel fand in drei Aussendungen statt, die die gebräuchlichsten Phishingangriffe simulierten (siehe auch die Tabelle „Lernziele des Live-Phishing-Trainings“auf der folgenden Seite).

Aussendung 1: Link auf vergiftete Website

In der ersten Aussendung des Live-Phishing-Trainings wurde den Mitarbeiterinnen und Mitarbeitern der Landeshauptstadt Kiel eine Phishing-E-Mail geschickt, die im Ernstfall versucht hätte, durch einen Drive-by-Exploit Schadsoftware auf dem Rechner der betreffenden Person zu installieren.

Der Text der Phishing-E-Mail der Kampagne simuliert eine mögliche, aber recht unwahrscheinliche Aktion der Finanzabteilung der Landeshauptstadt Kiel: Die Gehaltsmitteilung soll nicht mehr an die Büroadresse, sondern an die Heimanschrift gehen.

Die E-Mail enthält viele typische Kennzeichen von Spear-Phishing-E-Mails. Sie kann – wenn man vorbereitet

SiKoSH – Sicherheit für Kommunen in Schleswig-Holstein

„Sicherheit für Kommunen in Schleswig-Holstein“ (SiKoSH) ist ein Projekt des „Kommunalen Forums für Informationstechnik der Kommunalen Landesverbände in Schleswig-Holstein e. V.“ (KomFIT e. V.). Das KomFIT berät die kommunalen Landesverbände in verbandsübergreifenden IT-Angelegenheiten in den Themenbereichen E-Government, Informations- und Kommunikationstechnik und Informationssicherheit.

SiKoSH erarbeitet mit kommunalen Praktikern aus Schleswig-Holstein sowie Partnern aus anderen Bundesländern zahlreiche Hilfestellungen zum Aufbau eines nachhaltigen Informationssicherheitsmanagementsystems (ISMS) innerhalb von Kommunalverwaltungen. Fachlich wird das Projekt durch das Unabhängige Landeszentrum für Datenschutz (ULD), den Landesrechnungshof, Dataport und externe Berater unterstützt.

Alle Arbeitsergebnisse sind unter www.sikosh.de abrufbar und können unter Beachtung der Lizenzbedingungen auch von Behörden außerhalb Schleswig-Holsteins an die eigenen Bedürfnisse angepasst und intern weiter verwendet werden. Für Rückfragen steht SiKoSH unter sikosh@komfit.de zur Verfügung.