Informationssicherheit

Liebe Leserin, lieber Leser,

ohne die Unterstützung der Mitarbeiter kann sich heutzutage kein Unternehmen wirksam vor Cyberangriffen schützen. Als Datenschutzbeauftragter kennen Sie die täglichen Meldungen über großflächige Angriffe auf Unternehmen. Immer neue Trojaner oder Ransomware kommt zum Einsatz, ganze Netzwerke kommen zum Erliegen, weil Kriminelle die Server mit millionenfachen Anfragen zum Stillstand bringen. Milliarden Nutzerdaten werden bei Yahoo gestohlen.

Mangelnde Sensibilität führt dazu, dass ein Mitarbeiter eine Phishing-Mail öffnet oder Opfer eines Social Engineering-Angriffs wird. So öffnet der Mitarbeiter den Hackern die Tür in das Unternehmen.

Als Datenschutzbeauftragter ist es Ihre Aufgabe die Mitarbeiter zu schulen. Schulungen sind jedoch nur ein Baustein von vielen. Sie müssen zunächst die Aufmerksamkeit der Mitarbeiter erhalten. Eine Security Awareness-Kampagne schafft diese Aufmerksamkeit und ist das Fundament, auf dem Sie als Datenschutzbeauftragter mit weiteren Bausteinen eine Sicherheitskultur in Ihrem Unternehmen aufbauen können.

Lesen Sie jetzt wie Sie eine erfolgreiche Security Awareness-Kampagne aufbauen und konkret durchführen. Das ist eine fesselnde Aufgabe, bei der ich Ihnen viel Erfolg wünsche!

Security Awareness. Das müssen Sie jetzt wissen.

Angesichts der aktuellen Bedrohungslage durch Cyberkriminelle ist es für Unternehmen äußerst wichtig, die Mitarbeiter zu zentralen Themen der Datensicherheit – also Security Awareness aufzubauen - zu sensibilisieren. Mitarbeiter müssen eine aktive Haltung gegenüber Bedrohungen einnehmen. Dies ist nur zu erreichen, wenn Sie als Datenschutzbeauftragter aktiv für die Etablierung einer Sicherheitskultur in Ihrem Unternehmen eintreten..

Security Awareness wird seit vielen Jahren als Allheilmittel zur Verbesserung der Informationssicherheit propagiert. Als Datenschutzbeauftragter sollten Sie sich jedoch, zunächst darüber im Klaren sein, welche Ziele Sie verfolgen und mit welchen Methoden Sie diese Ziele in Ihrem Unternehmen erreichen können. Awareness-Kampagnen sind meist sehr zeitintensiv und in der Regel nicht ohne die Unterstützung externer Berater umzusetzen. Das kann sehr schnell sehr teuer werden.

Security Awareness 1.0. Aller Anfang ist schwer.

In den ersten Jahren standen bei Awareness 1.0 Schulungsmaßnahmen und der Einsatz von Web based Trainings (WBT) im Vordergrund. Die Mitarbeiter ließen sich von langweiligen Vorträgen berieseln und klickten sich durch Schulungsfolien. Die Lösungen zu den Prüfungsfragen kursierten im Unternehmen, Mitarbeiter erledigten die Trainings gegen ein Entgelt für die Kollegen. Die Erfolge solcher Awareness-Maßnahmen sind auch nicht messbar. In der betrieblichen Praxis hat sich gezeigt, dass solche Methoden für eine umfassende Sensibilisierung nicht ausreichend sind.

Security Awareness 2.0. So geht es weiter.

Als Konsequenz aus den Erfahrungen der Anfangszeiten wird versucht die Mitarbeiter über vielfältige Kommunikationskanäle zu erreichen. Das Mittel der Wahl sind Awareness-Kampagnen mit vielfältigen Sensibilisierungsmaßnahmen. Zentrale Botschaften werden durch Plakate, Flyer, Videos und Präsentationen im Unternehmen verbreitet. Ziel ist es die Mitarbeiter direkt anzusprechen und Aufmerksamkeit für zentrale Sicherheitsthemen zu erreichen. Es hat hat sich gezeigt, dass solchermaßen motivierte Mitarbeiter WBT-Maßnahmen mit deutlichen Lernerfolgen absolvierten.

Security Awareness 3.0. Im Zentrum steht das gesamte Unternehmen.

Awareness-Kampagnen haben gezeigt, dass sensibilisierte und motivierte Mitarbeiter nicht nur Informationen benötigen. Sicherheitsbewusstsein erfordert auch die Vermittlung von Lösungen. Mitarbeiter wollen klare Regelungen und klare Vorgaben für bestimmte sicherheitskritische Verfahren. So reicht es nicht aus, Mitarbeitern die Gefahren von Phishing-Angriffen aufzuzeigen. Mitarbeiter wollen wissen, wie Sie sich konkret verhalten müssen, wenn eine solche E-Mail in ihrem Postfach liegt. Es müssen also Richtlinien mit konkreten Vorgaben erstellt werden, die im gesamten Unternehmen verbindlich sind. Mitarbeiter fordern nämlich insbesonde-

re, dass sich auch Führungskräfte an solche Richtlinien halten. Als Datenschutzbeauftragter wissen Sie, dass gerade Geschäftsleiter gerne Sicherheitsrichtlinien in Frage stellen oder gar umgehen.

Fazit

Als Datenschutzbeauftragter sind Sie mit Awareness-Kampagnen der dritten Generation erfolgreich, wenn:

- *Sie ein Kampagnenkonzept haben, das die Mitarbeiter begeistert. Begeisterung ist eine der zentralen Voraussetzungen für das erfolgreiche Lernen.*
- *Sie den sensibilisierten Mitarbeitern Lösungen an die Hand geben, die es ihnen ermöglichen, Richtlinien einzuhalten ohne ihr Tagesgeschäft oder gar den Unternehmenserfolg negativ zu beeinflussen.*
- *Sie die Führungskräfte in die Verantwortung nehmen und darauf hinwirken, dass diese ihre Vorbild-funktion wahrnehmen. Hierzu zählt auch, dass die Führungskräfte sich gegenüber ihren Mitarbeitern eindeutig zu den Unternehmensrichtlinien bekennen und diese nachvollziehbar einhalten.*

Lesen Sie auf den folgenden Seiten, wie Sie Mitarbeiter begeistern, wie Sie Fehler vermeiden und ob Security Awareness 3.0 wirklich alle Risiken aktueller Bedrohungen adressieren kann.

Sicherheitskultur. Diese Definition müssen Sie kennen.

Der Begriff Sicherheitskultur ist gerade in der heutigen Zeit in aller Munde. Als Datenschutzbeauftragter sollten Sie sich die folgende Definition aus Wikipedia zu Eigen machen. Sicherheitskultur ist nach Wikipedia ein Verhaltensmerkmal einer Gruppe oder Organisation wie mit Fragen zur Sicherheit umgegangen wird. Es unterliegt einem komplexen Lernprozess, in dem sich gemeinsame Ziele, Interessen, Normen, Werte und Verhaltensmuster herausbilden. Diese Definition lässt sich problemlos auf Fragen zur Informationssicherheit anwenden.

Sicherheitskultur und Unternehmenskultur. Das eine geht nicht ohne das andere.

Security-Spezialisten meinen, eine Sicherheitskultur im Unternehmen sei unabdinglich. Viele Anbieter von Security Awareness-Kampagnen behaupten, dass die Sicherheitskultur gefördert werden muss.. Eine Sicherheitskultur muss jedes Unternehmen haben, das ist richtig. Diese Sicherheitskultur muss aber zu dem Unternehmen passen und Teil der Unternehmenskultur sein. Nur dann kann dieser komplexe Lernprozess, in Ihrem Unternehmen erfolgreich sein. Das Resultat dieses Lernprozesses ist eine Informationssicherheitskultur. Als Datenschutzbeauftragter müssen Sie sich immer vor Augen führen, dass alle Maßnahmen und Richtlinien zu der Unternehmenskultur Ihres Unternehmens passen müssen.

Mein Tipp

Beschäftigen Sie sich als Datenschutzbeauftragter intensiv mit Ihren Kollegen im Unternehmen. Finden Sie heraus welche ungeschriebenen Gesetze es gibt, wie die Mitarbeiter untereinander kommunizieren, was auf dem Flurfunk besprochen wird und welche Themen kritisch diskutiert werden. Setzen Sie sich in der Kantine zu Mitarbeitern, die Sie noch nicht kennen, reden Sie an der Kaffeebar mit Kollegen über aktuelle Themen im Unternehmen. Präsentieren Sie sich als Kollege, nicht als Datenschutzbeauftragter. Sie werden sehen, dass Sie Ihre Kollegen ganz anders wahrnehmen und auch ganz anders wahrgenommen werden. Nur wenn Sie einschätzen können wie die Mitarbeiter im Unternehmen kommunizieren, werden Sie als Datenschutzbeauftragter für Ihre Themen auf offene Ohren stoßen.

Paranoid oder effizient? Das müssen Sie über Ihr Unternehmen wissen.

Die Aussage „wir haben eine echte Sicherheitskultur“ kann unterschiedlichste Assoziationen hervorrufen. Manche denken daran, dass paranoide Datenschützer und Sicherheitsexperten alle IT-Systeme so abgesichert haben, dass das Tagesgeschäft eine Qual ist. Andere denken an effiziente Sicherheitsprozesse, an IT-Systeme, die wirksam vor Angriffen schützen, aber die Mitarbeiter bei Ihrer Arbeit nicht behindern. Als Datenschutzbeauftragter sollten Sie auf keinen Fall der Paranoia verfallen, auch wenn es nicht immer leicht ist. Eine wirksame Sicherheitskultur können Sie nur etablieren, wenn Sie auf die nachfolgenden grundsätzlichen Verhaltensweisen vorbereitet sind und in Erfahrung bringen, wie diese Verhaltensweisen in Ihrem Unternehmen ausgeprägt sind.

Dynamik. Was machen denn die Kollegen?

Sie werden als Datenschutzbeauftragter dafür gesorgt haben, dass jeder neue Mitarbeiter Unterlagen mit den wichtigsten Richtlinien, Maßnahmen zur Informationssicherheit wie z.B. Verschlüsselung, Virenschutz usw. erhält. Auch ein Flyer zum Datenschutz und die Einladung zum Web based Training sollte nicht fehlen. Aber Sie müssen auch abschätzen können, was dieser neue Mitarbeiter von seinen Kollegen im Büro erfährt. Wird er dort erfahren, dass er den ganzen „Sicherheitsquatsch“ vergessen kann? Wird man ihm gleich zeigen, wie er die Vorschriften umgehen kann? Sie dürfen als Datenschutzbeauftragter diese Dynamik nicht unterschätzen. Diese Dynamik zu durchbrechen ist das zentrale Element einer erfolgreichen Awareness-Kampagne.

Beharrlichkeit. Das haben wir doch schon immer so gemacht.

In einem Unternehmen gibt es Praktiken, die seit Generationen an jeden neuen Mitarbeiter weitergegeben werden. Hierzu gehört z.B., dass Rechner nicht mit Passwörtern gesichert werden („das nervt nur!“), E-Mails mit vertraulichen Kundendaten nicht verschlüsselt werden („viel zu kompliziert, das kann eh jeder lesen“), Büroschränke nicht verschlossen werden („was soll der Aufwand, das interessiert doch keinen“) und so weiter. Als Datenschutzbeauftragter werden Sie weitere Beispiele aus Ihrer täglichen Praxis kennen. Um dieses Beharrungsvermögen in Ihrem Unternehmen aufzubrechen, müssen Sie die zu ändernden Praktiken exakt benennen und konkrete Alternativen vorgeben.

Mein Tipp
Vermeiden Sie unbedingt, die „aus guten Gründen" gelebten Praktiken abschätzig zu bewerten. Schließlich ist es Ihr Ziel die Mitarbeiter zu überzeugen, ihre lieb gewonnenen Praktiken durch neue zu ersetzen und nicht die Mitarbeiter herabzusetzen.

Trotz. Das sehe ich ja gar nicht ein.
Als Datenschutzbeauftragter müssen Sie damit rechnen, dass Mitarbeiter sehr sensibel darauf reagieren, wenn Maßnahmen ihre Handlungsfreiheit einschränken oder einfach nach ihrem eigenen Erfahrungsschatz inakzeptabel erscheinen. Sie müssen sich also intensiv damit auseinandersetzen „WIE" Sie Ihre Maßnahmen kommunizieren. Sie müssen für Ihre Ziele werben und nicht als Despot auftreten, der die „Weisheit gepachtet" hat. Sie müssen überzeugen und die Kollegen begeistern. Das erreichen Sie nur mit sehr viel Einfühlungsvermögen, Geduld und Überzeugungskraft. Andernfalls laufen Sie Gefahr, dass Ihre Maßnahmen als Willkürakt angesehen werden und unterschwellige aber oft nachhaltige Gegenwehr auslösen.

Security Awareness 4.0. So gehen Sie konkret vor.

Awareness-Kampagnen zielen in erster Linie darauf ab auf unterschiedlichsten Kommunikationskanälen Mitarbeiter auf ein Thema aufmerksam zu machen und zum Handeln zu bewegen. Hierbei kommen Plakate, Flyer, Videos und Trainings zum Einsatz. Zum Erreichen maximaler Aufmerksamkeit werden auch gezielte Attacken auf die Mitarbeiter mit gefälschten E-Mails ausgeführt. In weiteren Szenarien geistern vermeintliche Spione durchs Unternehmen, die unachtsamen Mitarbeitern z.B. vertrauliche Informationen entwenden. In den letzten Jahren hat sich gezeigt, dass es für den nachhaltigen Erfolg einer Awareness-Kampagne unerlässlich ist, diese bewährten aber zumeist einmaligen Maßnahmen mit längerfristigen Methoden zu unterstützen.

Die Bedeutung der Mitarbeitersensibilisierung nimmt in Zeiten von massiven Angriffen auf Unternehmen stetig zu. Um dieser Bedeutung gerecht zu werden, müssen Sie ausgetretene Pfade verlassen. Setzen Sie auf Bewährtes, aber reichern Sie es mit neuen Methoden an. Sie müssen als Datenschutzbeauftragter darauf hinwirken, dass sich Ihr Unternehmen diesen Herausforderungen stellt und eine nachhaltige Sicherheitskultur etabliert werden kann.

Zielsetzung. Definieren Sie Ihre Ziele.
Eine Awareness-Kampagne kann nur erfolgreich sein, wenn die Ziele konkret definiert sind. Andernfalls werden Sie bei den Mitarbeitern das Gefühl von Beliebigkeit erzeugen, aber Sie werden niemanden begeistern können. Ohne konkrete Ziele ist der Erfolg einer Awareness-Kampagne auch nicht messbar. Konkret könnten Sie sich das Ziel setzen die Mitarbeiter für die folgenden Themen zu sensibilisieren:

- Social Engineering
- Trojaner und Ransomware
- E-Mailsicherheit

Sie möchten zudem den Erfolg der Awareness-Kampagne messen und nachhaltige Maßnahmen zur Etablierung einer Sicherheitskultur etablieren.

Bestandteile der Awareness-Kampagne. Das müssen Sie planen.
Sie müssen bei der Planung einer Awareness-Kampagne Vieles beachten. Zunächst sollten Sie sich darüber im Klaren sein, dass eine solche Kampagne ohne die Unterstützung der Geschäftsleitung nicht sinnvoll ist. Nur wenn Ihre Geschäftsleitung sich klar und deutlich zu den Inhalten der Awareness-Kampagne bekennt und Sie unterstützt, können Sie beginnen. Neben der Kommunikation mit den Mitarbeitern müssen Sie sich mit den folgenden Bestandteilen einer Awareness-Kampagne auseinandersetzen:

1. Aussagekräftiger Kampagnen-Slogan und Logo
2. Initiale Awareness-Aktion.
3. Rundschreiben oder E-Mail der Geschäftsleitung (Management-Attention)
4. Start der Kampagne mit Werbeträgern (Plakate, Flyer, Intranetseite usw.)
5. Präsentationen zu den Themen (eventuell mit Live Hacking Beiträgen)
6. Zielgruppenorientierte Trainings (HR, IT, Manager, Alle Mitarbeiter)
7. Methoden zur Erfolgsmessung

Der Slogan. Das zentrale Element Ihrer Kampagne.
Eine Awareness-Kampagne benötig zunächst einen aussagekräftigen Slogan und falls möglich ein Logo. Beide Elemente sollten so gewählt werden, dass sie zur Identität Ihres Unternehmens passen und in der Zukunft auf Ihren Veröffentlichungen (Rundschreiben, E-Mails, Intranetseiten) verwendet werden können. So erreichen Sie einen nachhaltigen Wiedererkennungseffekt, der auch dazu führt dass die Inhalte der Kampagne bei den Mitarbeitern in Erinnerung bleiben. Konkrete Beispiele zu Slogans:
„Sie sind der wichtigste Mitarbeiter der IT-Sicherheit".
„Ihre Weitsicht, unsere Sicherheit"
„Unsere Mitarbeiter sind unsere stärkste Firewall"
„Sie trotzen jedem Angriff. Mit SICHERHEIT"

Mein Tipp
Mit solchen Slogans können Sie Mitarbeiter erreichen. Sie signalisieren den Mitarbeitern, dass Ihr Unternehmen die Mitarbeiter wertschätzt und auf sie baut. So verhindern Sie Trotzreaktionen und gehen gleichzeitig gegen die Beharrlichkeit einiger Kollegen vor. Setzen Sie sich mit Ihrer Marketingabteilung in Verbindung. Die Kollegen kennen bestimmt einen Grafiker, der Ihnen zu Ihrem Slogan ein Logo entwirft.

Die Phishing Mail. So gehört alle Aufmerksamkeit Ihrer Kampagne.

Bis jetzt haben Sie als Datenschutzbeauftragter Ihre Geschäftsleitung davon überzeugt, dass eine Security Awareness-Kampagne für die Sicherheit im Unternehmen sehr wichtig ist. Sie haben ein Budget mit dem Sie zumindest die begleitenden Maßnahmen wie Flyer, Plakate, Sticker, Gestaltung des Logos usw. finanzieren können. Bestenfalls haben Sie noch ein Budget für externe Unterstützung durch externe Fachkräfte. In Ihrem Unternehmen ist von Ihren Planungen noch nichts bekannt geworden. Das sollte auch so bleiben. Denn jetzt müssen Sie den Paukenschlag vorbereiten, mit dem Sie Ihre Kampagne starten. Damit dieser Start gelingt, müssen Sie die volle Aufmerksamkeit Ihrer Mitarbeiter haben.

Als Paukenschlag hat sich bewährt einen Phishing-Angriff per E-Mail nachzubilden. Hierzu müssen Sie sich zunächst ein Szenario ausdenken, mit dem Sie die Mitarbeiter ködern können. Versuchen Sie ein realistisches Szenario zu finden, das zu Ihrem Unternehmen passt. Das kann z.B. der Umstand sein, dass in Ihrem Unternehmen neue Smartphones eingeführt werden. Konkret können Sie diesen Umstand wie folgt für Ihre Kampagne nutzen.

Das Szenario. So bereiten Sie Ihren Paukenschlag vor.
Bereiten Sie eine E-Mail vor in dem Sie nachfolgendes Szenario beschreiben:
Im Unternehmen sollen iPhones eingeführt werden. Die IT-Abteilung sucht nun Mitarbeiter, die bereit sind die neuen Geräte auf Herz und Nieren zu testen. Die Testpersonen können die iPhones als Dankeschön am Ende des Tests behalten. Da nur eine begrenzte Anzahl von Testgeräten bereit steht, werden die Teilnehmer ausgelost. Die Interessenten müssen sich auf der Internetseite des Unternehmens mit ihrem Benutzeraccount und Passwort registrieren.

Im nächsten Schritt müssen Sie eine Internetseite bereitstellen, die das oben aufgeführte Szenario abbildet. Auf dieser Seite muss ein Eingabefeld für einen Benutzernamen und ein Passwort vorhanden sein. Die Anzahl der Besucher der Internetseite und die Anzahl der Mitarbeiter, welche die Anmeldung durchgeführt haben, muss gespeichert werden. Haben Sie Unterstützung durch ein Beratungshaus, wird eine solche Seite in der Regel bereitgestellt. In diesem Fall muss sichergestellt werden, dass die Eingaben der Mitarbeiter nicht gespeichert werden. Sorgen Sie dafür, dass Ihre Internetseite auf deren Server nachgebildet wird. So hat das Ganze einen authentischen Hintergrund. Müssen Sie ohne die Unterstützung eines Beratungshauses auskommen, sollten Sie einen Kollegen der IT-Abteilung zu Ihrem „Komplizen" machen. Er kann Ihnen dabei helfen, solche Phishing Mails mit einem kostenfreien Tool im Internet zu erstellen.

Mein Tipp
Bevor Sie Ihren „Angriff" per E-Mail starten, müssen Sie als Datenschutzbeauftragter Ihre IT-Abteilung und den Betriebsrat informieren. Die Kollegen aus der IT müssen darauf vorbereitet sein, dass Mitarbeiter beim Support nachfragen, was denn das für ein Test sei usw. Den Betriebsrat müssen Sie darüber informieren, dass Sie lediglich Aufmerksamkeit für die Kampagne erreichen wollen, dass ausschließlich anonymisierte Daten gespeichert werden und keine personenbezogenen Auswertungen gemacht werden.

Die E-Mail. So täuschen Sie die Mitarbeiter.
Wenn die E-Mail sprachlich zu Ihrem Unternehmen passt und sich inhaltlich auf ein reales allgemein bekanntes Thema bezieht, werden in der Regel die meisten Mitarbeiter in die Falle tappen. Um das Szenario zu verschärfen, sollten Sie die Absenderadresse Ihres IT-Supportes leicht verfälschen und in der Mail darauf hinweisen, dass es sich um eine Fälschung handelt, dass es keine Tests gibt und dass man auf keinen Fall seinen Benutzernamen und sein Passwort auf einer Internetseite eingeben soll. Schreiben Sie diesen Text an das Ende der Mail in Schriftgröße 3 oder 4 und ändern Sie z.B. die Absenderadresse „IT-Support@muster.de" in „IT-Suport@muster.de". So können Sie bei der Auswertung anschaulich verdeutlichen, wie leicht es ist E-Mailadressen zu fälschen, und wie leicht sich Menschen von einem vermeintlichen tollen Angebot ablenken lassen. Allein die Attraktivität des Angebotes entscheidet darüber, ob die gefälschte E-Mailadresse und die Fußzeile der Mail von einem Mitarbeiter wahrgenommen werden.

Haben Sie alles vorbereitet, sollten Sie als Datenschutzbeauftragter die Mitarbeiter der IT-Abteilung und insbesondere die Kollegen an der IT-Hotline über die Aktion informieren. Machen Sie den Kollegen klar, dass sie den Mitarbeitern, die sich über die Hintergründe der E-Mail informieren wollen, keine direkten Auskünfte zu der Kampagne geben. Natürlich dürfen sie auch nicht bestätigen, dass die E-Mail echt ist. Am besten ist es, wenn die Kollegen des IT-Supportes einfach aussagen, dass sie die Hintergründe klären müssen und sich dann wieder melden. Für die Statistik ist es wichtig, dass die Anzahl der Anrufer festgehalten wird. Weisen Sie als Datenschutzbeauftragter darauf hin, dass keine Namen registriert werden dürfen. Nach diesen Vorbereitungen können Sie die E-Mail an alle Mitarbeiter senden.

Mein Tipp
Werten Sie die Ergebnisse am gleichen Tag aus. Dass mit dieser E-Mail irgendetwas nicht stimmt, wird sich schnell in Ihrem Unternehmen verbreiten. Nachzügler sind daher meist informiert und verfälschen das Bild.

Kampagnenbeginn. So beginnen Sie richtig.
Nach dem Versand der E-Mail sollten Sie unmittelbar am darauffolgenden Tag mit der Kampagne starten. Lassen Sie die Plakate am vorhergehenden Abend - nach Büroschluss - aufhängen und verteilen Sie die Flyer in den Büroräumen. Sie müssen die Mitarbeiter möglichst überraschen. Lassen Sie die E-Mail der Geschäftsleitung daher auch am Vorabend versenden. In dieser E-Mail sollte die Geschäftsleitung die Kampagne kurz vorstellen, die gemeinsamen Ziele hervorheben und die zentrale Rolle der Mitarbeiter hervorheben.

Wenn möglich sollten Sie am Morgen des Kampagnenstarts am zentralen Unternehmenseingang präsent sein. Verteilen Sie die Sticker mit dem Logo oder den Slogans an die Mitarbeiter. So machen Sie auf die Kampagne aufmerksam, machen die Mitarbeiter neugierig und machen sich als Kopf der Kampagne bekannt

Für die Flyer haben sich Themen wie „So erstellen Sie ein sicheres Passwort" oder die „10 goldenen Regeln der Datensicherheit" bewährt.

Mein Tipp
Jede erfolgreiche Kampagne benötigt ein bekanntes „Gesicht" aus dem Hause als Werbeträger. Das erleichtert es den Mitarbeiter sich mit der Kampagne zu identifizieren. Gleichzeitig ist dieses Gesicht auch die Integrationsfigur für die Mitarbeiter. Denn es fällt schwerer sich von einem Thema abzuwenden, wenn dieses Thema von einem Menschen besetzt ist, den man im Unternehmen kennt und vielleicht sogar schätzen gelernt hat. Als Datenschutzbeauftragter können Sie Ihrer Awareness-Kampagne so ein Gesicht geben.

Präsentationen. So präsentieren Sie richtig.
Präsentationen zu Awareness-Kampagnen müssen zentrale Botschaften und kein Fachwissen vermitteln. Fachwissen wird in Trainingseinheiten vermittelt. Diese werden im späteren Verlauf der Awareness-Kampagne durchgeführt. Verwenden Sie daher in Ihren Präsentationen viel Bildmaterial, Comicfiguren, Videos und wenig Text. Sie müssen die Mitarbeiter begeistern und nicht langweilen. Videos, Bilder und Vorlagen für Präsentationen können Sie bei spezialisierten Anbietern im Internet beziehen. Zum Teil auch kostenlos. Bewährt haben sich auch kleine Live Hacking Beiträge, bei denen z.B. gezeigt wird, wie schnell Passwörter gehackt werden oder wie leicht man mit einem USB-Stick Daten ausspionieren kann. Auf den folgenden Seiten finden Sie hierzu konkrete Beispiele, die Sie direkt nutzen können.

Mein Tipp
Zu den Präsentationsterminen sollten alle Mitarbeiter eingeladen werden. Wirken Sie darauf hin, dass die Geschäftsleitung vor jeder Präsentation zu den Mitarbeitern spricht und sich für die Ziele der Awareness-Kampagne stark macht. Die Anwesenheit des Managements ist für den Erfolg der Awareness-Kampagne von entscheidender Bedeutung. Stecken Sie der Geschäftsleitung zu Beginn des Vortrages einen Button an. Das lockert die Stimmung auf und sorgt für Solidarität mit den Mitarbeitern.

Stellen Sie auf einer Folie die Ergebnisse der Phishing-Mail dar. Heben Sie hervor wieviel Prozent der Mitarbeiter den Link in der Mail angeklickt haben und wie viele Mitarbeiter tatsächlich ihren Benutzernamen und ihr Passwort eingegeben haben. Weisen Sie aber darauf hin, dass dieses Ergebnis normal ist. Verdeutlichen Sie, dass es menschlich ist, seiner Neugierde nachzugeben und solchen vermeintlich attraktiven Angeboten reflexartig nachzukommen. Zeigen Sie Solidarität, vermeiden Sie den Oberlehrer und weisen Sie darauf hin, dass Sie auch schon in solche Fallen getappt sind. Bisher zum Glück nur im privaten Bereich und ohne große Folgen. So können Sie die Mitarbeiter sensibilisieren und in die Awareness-Kampagne mitnehmen. Denken Sie immer daran, dass Sie gegen die Beharrlichkeit und den Trotz der Mitarbeiter kämpfen müssen. Da hilft es nicht mit Fachwissen zu glänzen. Ein Lacher und ein gut gemachtes Video, das die Zuschauer fesselt, sind bei weitem hilfreicher.

Training. So erreichen Sie die Mitarbeiter.
Sie haben die Mitarbeiter mit Ihrer Phishing-Mail aufgerüttelt, Plakate und Buttons verteilt und Ihre Vorträge bei gut besuchten Veranstaltungen gehalten. Ihre Security Awareness-Kampagne war ein voller Erfolg und die Mitarbeiter unterhalten sich noch immer über diese tolle Awareness-Kampagne. Nun gilt es aber, diese Aufmerksamkeit zu nutzen um den Mitarbeitern Ihre zentralen Themen nachhaltig zu vermitteln. Um dieses Ziel zu erreichen, müssen Sie zielgruppenorientierte Trainings durchführen. Zielgruppen sind in der Regel „alle Mitarbeiter“, „Führungskräfte“ und „Geschäftsleitung“. Neben diesen primären Zielgruppen sollten Sie Trainings zu speziellen Business Themen wie z.B. Personaldaten, Kundendaten, Forschungsdaten sowie Ergänzungstrainings zu Sicherheitsthemen planen.

Web based Training. Das sind die Anforderungen.
Für die Zielgruppe „Alle Mitarbeiter“ können Sie nur in kleinen Unternehmen Präsenztrainings anbieten. Ab einer Größenordnung von 100 Mitarbeitern ist der Einsatz eines Web based Trainings (WBT) sinnvoller. Achten Sie bei der Auswahl eines Produktes darauf, dass dabei mit Multimedia Inhalten (Videos, Animationen, Comicelemente, Sprache usw.) gearbeitet wird und eine Erfolgskontrolle oder ein Test integriert sind.

Mein Tipp
Das Training muss kurzweilig und interessant sein. Die Mitarbeiter müssen das WBT aufrufen, weil es Ihnen Spaß macht. Nur so können Sie vermeiden, dass das WBT als lästige Pflichtübung verstanden wird und die Lösungen für die Testfragen im Unternehmen kursieren, weil jeder das WBT schnell durchklicken will. Ein langwei-

liges WBT oder ein WBT in dem mit dem erhobenen Zeigefinger gearbeitet wird, kann Ihnen die Erfolge Ihrer gesamten Security Awareness-Kampagne zunichtemachen. Legen Sie großen Wert darauf, dass das WBT auf Ihr Unternehmen passt. Dazu gehört auch die richtige Kommunikation bei der Vermittlung der Lerninhalte.

In der Regel können diese Programme auf die CI des Unternehmens angepasst werden. Sie sollten die Slogans und Logos Ihrer Awareness-Kampagne in das WBT integrieren. So schaffen Sie einen Wiedererkennungswert und beugen einer Abwehrhaltung der Mitarbeiter vor.

Mein Tipp
Das WBT sollte einen Pool von Fragen bereitstellen und nach einem Zufallsprinzip eine bestimmte Anzahl von Fragen für den Teilnehmer auswählen. Das WBT sollte nicht länger als eine Stunde dauern und es muss die Möglichkeit bestehen, dass der Teilnehmer das WBT an beliebigen Stellen wiederaufnehmen kann. Der Teilnehmer muss auch den Test so lange wiederholen können, bis er alle Fragen beantwortet hat. Am Ende sollte ein Zertifikat mit Ihrem Kampagnenlogo ausgedruckt werden. Dieses Zertifikat sollte in die Personalakte. Damit verdeutlichen Sie dem Mitarbeiter, wie wichtig dieses Training ist.

Das WBT sollte alle zwei Jahre wiederholt und aktualisiert werden. Neue Mitarbeiter sollten das WBT innerhalb des ersten Monats absolviert haben. Als Datenschutzbeauftragter müssen Sie vor Einführung des WBT den Betriebsrat informieren und darauf hinwirken, dass keine personenbezogenen Daten der Mitarbeiter in dem WBT gespeichert und verarbeitet werden. Das WBT darf nicht der Leistungskontrolle dienen.

Führungskräfte. Training für die Vorbilder.
Führungskräfte müssen ein Bewusstsein dafür entwickeln, das Sie eine besondere Verantwortung für das Thema Sicherheit tragen. Sie müssen den Mitarbeitern ein Vorbild sein und die Mitarbeiter immer wieder dazu ermutigen die Sicherheitsrichtlinien einzuhalten und sich bei der täglichen Arbeit die erforderliche Sensibilität und Aufmerksamkeit für die Informationssicherheit zu bewahren. Führungskräfte müssen geschult werden, damit Sie:

- wie alle Mitarbeiter die Sicherheitsrichtlinien einhalten
- den Mitarbeitern als Vorbild dienen können
- in ihrem Fachbereich Verantwortung für die Informationssicherheit übernehmen
- in ihrer Personalverantwortung auch den Datenschutz ernst nehmen.

Je nach Unternehmensgröße bieten sich Präsenztrainings für Führungskräfte an oder WBTs mit den genannten Inhalten. In beiden Fällen sollten die Trainings nicht länger als 20 Minuten dauern. Auch bei diesem Training ist es wichtig auf Unterhaltung zu setzen. Das Training sollte von allen Führungskräften alle zwei Jahre wiederholt werden. Neue Führungskräfte sollten das Training bei Aufnahme Ihrer Führungstätigkeit absolvieren.

Fachbereiche. Diese Themen sollten Sie schulen.
In den einzelnen Fachbereichen werden spezielle Anforderungen an die Informationssicherheit und den Datenschutz gestellt. Hier ist Ihre Erfahrung als Datenschutzbeauftragter gefragt. Sie sollten Ihr Unternehmen kennen und wissen, welche Abteilungen mit sensiblen Daten arbeiten und welche Anforderungen darin umzusetzen sind. So müssen Sie in der Personalabteilung großen Wert auf die Vermittlung datenschutzrechtlicher Anforderungen legen. Im Kundenbereich geht es eher darum, die Mitarbeiter dahingehend zu sensibilisieren, dass die Kundendaten vertraulich zu behandeln.

Mein Tipp
Erstellen Sie eine Liste mit Fachbereichen und erfassen Sie die Informationen, die in den jeweiligen Fachbereichen verarbeitet werden. Entwickeln Sie für jeden Fachbereich Trainingsinhalte, die zu den Informationen passen, die dort verarbeitet werden. So erhalten Sie sehr schnell die richtigen Trainingsinhalte für die jeweiligen Fachbereiche.

Beispiel zielgruppenorientierte Trainingsinhalte

Fachbereich	Informationen	Trainingsinhalte
Personal	Mitarbeiterdaten, Gesundheitsdaten, Personalakten	Beschäftigtendatenschutz, Vertraulichkeit, Aufbewahrungsfristen, Clean Desk, Sicherer Austausch von Daten, Verschlüsselung, Aktenvernichtung
Verkauf, Akquise	Kundendaten	Datenschutz allgemein, Einwilligungserklärungen, Telefonmarketing, Sicherheit auf Reisen, Vertraulichkeit, Verschlüsselung
Marketing	Kundendaten, Unternehmensdaten	Datenschutz allgemein, Einwilligungserklärungen, Widerrufsbelehrungen, Datenschutzgerechter Internetauftritt, Telefonmarketing, E-Mailsicherheit
IT	Mitarbeiterdaten, Kundendaten, Protokolldaten, Verbindungsdaten	Datenschutz allgemein, TOMs, Vertraulichkeit, TKG, TMG, IT-Sicherheitsgesetz, Sicherheitsvorfallbehandlung, Datenträgervernichtung, Verschlüsselung, Mobile Security

Erfassen Sie alle Fachbereiche in Ihrem Unternehmen. Sie werden feststellen, dass es viele sich überschneidenden Themenbereiche gibt. Diese gemeinsamen Themen können Sie als Grundlage für den allgemeinen Teil der Trainings ausarbeiten. Die Spezialthemen sollten Sie dann für die jeweiligen Fachbereiche individuell ausarbeiten.

Mein Tipp

Nehmen Sie in den allgemeinen Teil Ihres Trainings die folgenden Themen auf:

- *mobile Sicherheit (Smartphones)*
- *Sicherheit auf Reisen (Transport von Notebooks, Aktenkoffern usw.)*
- *sicherer Datenaustausch*
- *E-Mailsicherheit*
- *Internetsicherheit*
- *Phishing*
- *Social Engineering*
- *Malware (Trojaner, Ransomware usw.)*

Mit diesen Themen haben Sie ein ausreichendes Spektrum an Themen für Ihre Sicherheitstrainings.

Geschäftsleitung. So führen Sie die richtigen Events durch.

Sie haben sich als Datenschutzbeauftragter bestimmt schon die Frage gestellt, wie Sie die Geschäftsleitung dazu bewegen können an Trainings teilzunehmen. In der Regel stoßen Sie zwar auf grundsätzliches Interesse an den Themen, aber Sie scheitern meist an zeitlichen Hürden. Sie sollten an dieser Stelle auf externe Sicherheitsexperten zurückgreifen. Diese Profis veranstalten Live Hacking-Events mit Topmanagern. Ziel ist es, die Themen von Sicherheitsexperten einem ausgesuchten Kreis in einer spannenden Showveranstaltung zu präsentieren. Solche Events rütteln die Manager auf und machen sie persönlich betroffen. Sie haben nach einem solchen Event als Datenschutzbeauftragter die volle Aufmerksamkeit für Ihre Themen.

Mein Tipp

Planen Sie solche Events bereits bei Ihrer Budgetplanung für die Awareness-Kampagne ein. Dann müssen Sie Ihre Geschäftsleitung nicht gesondert von dem Nutzen einer solchen Veranstaltung überzeugen. Lassen Sie die Veranstaltung filmen und in Ihrem Intranet für alle Mitarbeiter bereitstellen. Am besten mit einem Begleitwort Ihrer Geschäftsleitung.

Erfolgsmessung. Das müssen Sie umsetzen.
Nachdem Sie Ihre Geschäftsleitung mit einem Live Hacking-Event sensibilisiert haben, gilt es den Erfolg der Security Awareness-Kampagne nachzuweisen. Erfolgsmessungen machen transparent, ob Sie mit Ihren Sensibilisierungsmaßnahmen gegen die Dynamik, die Beharrlichkeit und Trotz der Mitarbeiter erfolgreich waren und ob in den Trainings nachhaltig Fachwissen vermittelt wurde. Aus den Ergebnissen können Sie direkt erkennen an welchen Themen Sie weiterarbeiten müssen. Spätestens jetzt wird deutlich, dass Ihre Aufgabe nicht mit der Durchführung einer Security Awareness-Kampagne beendet ist. Diese Awareness-Kampagne war der erste Schritt auf Ihrem Weg zur Etablierung einer Sicherheitskultur auf dem Sie die gemeinsamen Ziele, Interessen, Normen, Werte und Verhaltensmuster in Ihrem Unternehmen herausbilden müssen.

Die Auswertung der Phishing-Mail hat Ihnen sehr genau gezeigt wie viele Mitarbeiter anfällig für solche Angriffe sind. Wenn Sie einen solchen Angriff ein halbes Jahr nach Ihrer Awareness-Kampagne wiederholen, haben Sie einen deutlichen Nachweis, ob sich die Aufmerksamkeit Ihrer Mitarbeiter verbessert hat. Ebenso liefert Ihnen das WBT in der Regel Informationen darüber, wie viele Mitarbeiter teilgenommen haben und wie deren Testergebnisse waren. Auch hier können Sie durch regelmäßige Auswertungen erfahren wie der Kenntnisstand Ihrer Mitarbeiter ist. Führen Sie als Datenschutzbeauftragter weitere Prüfungen durch, mit denen Sie messbare Ergebnisse erhalten. Erstellen Sie einen Prüfungsplan mit dem Sie den Erfolg Ihrer Maßnahmen nachweisen können.
Beispiel Prüfungsplan.

Prüfung	Methode	Prüfungsgegenstand
Phishing-Mail	Versand einer gefälschten Mail an alle Mitarbeiter	Sensibilität der Mitarbeiter
Web based-Training	Durchführung Lernprogramm	Vorhandensein von Fachwissen
Social Engineering	Kontrollanrufe in Fachabteilungen. Aufforderung zur Herausgabe vertraulicher Informationen	Sensibilität der Mitarbeiter
Sicherheitsmeldungen	Auswertung der Help Desk Datenbank. Anzahl der Nachfragen zu auffälligen E-Mails, Internetseiten oder Auffälligkeiten bei der Nutzung von Programmen)	Sensibilität der Mitarbeiter
Clean Desk	Vor Ort-Prüfung. Rundgang durch das Unternehmen	Einhaltung von Richtlinien. Sensibilität der Mitarbeiter
E-Mailverschlüsselung	Auswertung der E-Mailprotokolle. Anzahl verschlüsselter E-Mails	Einhaltung von Richtlinien. Sensibilität der Mitarbeiter

Fazit
Mit solchen Prüfungen können Sie über einen längeren Zeitraum auswerten, ob sich das Verhalten der Mitarbeiter durch Ihre Awareness-Maßnahmen ändert. Stellen Sie Verbesserungen fest, sollten Sie diese auch kommunizieren. Ihrer Geschäftsleitung können Sie nachweisen, dass sich die Security Awareness-Kampagne bezahlt gemacht hat und die Mitarbeiter können Sie für ihre Sensibilität und ihr Fachwissen loben. Verschlechtern sich die Ergebnisse, müssen Sie themengerecht Trainings- oder Sensibilisierungsmaßnahmen durchführen. So können Sie sehr genau steuern, in welchen Themenbereichen Sie aktiv Maßnahmen ergreifen müssen.

Awareness 4.0. Das fehlt Ihnen noch zum Erfolg.

Der bisherige Aufbau der Awareness-Kampagne ist geprägt davon das Verhalten der Mitarbeiter durch konkrete Vorgaben zu beeinflussen. Auch in Trainings wird in der Regel für jede Zielgruppe konkretes Fachwissen vermittelt. Diese Methodik setzt darauf, dass die Sicherheitsexperten oder Datenschutzexperten wissen, welche Verhaltensweisen die Mitarbeiter haben, welche es zu ändern gilt und über welchen Wissensstand diese Mitarbeiter verfügen. Leider ist diese Methodik aber in der Regel nicht von Erfolg gekrönt. Deshalb werden in solchen Awareness-Kampagnen gerade die kritischen Zielgruppen wie z.B. IT-Personal, Manager, Programmierer und Medienprofis nicht erreicht. Solche Zielgruppen haben in der Regel eine sehr hohe Fachkompetenz und oftmals auch eine akademische Ausbildung. Hier stößt man immer wieder auf Beharrlichkeit und Trotz in Bezug auf Sicherheitsthemen.

Sie müssen als Datenschutzbeauftragter bei solchen Zielgruppen auch beachten, dass diese in der Regel in ihrer täglichen Praxis direkt mit Fragen zur Geheimhaltung, Sicherheit und dem Risikomanagement konfrontiert werden. Demnach können gerade diese Zielgruppen Ihre Kernaufgaben nur dann erfüllen, wenn Sie über ein ausreichendes Wissen in der Informationssicherheit verfügen und dieses auch anwenden.

Mein Tipp
Veranstalten Sie offene Diskussionsgruppen in denen Sie konkrete Anforderungen mit den Zielgruppen besprechen. Geben Sie den Mitarbeitern die Gelegenheit ihre Einschätzung der Bedrohungslage und ihre konkreten Maßnahmen vorzutragen. Schätzen Sie diese Maßnahmen objektiv ein und identifizieren Sie bei Bedarf gemeinsam Verbesserungspotentiale. Sie werden feststellen, dass die Mitarbeiter in der Regel über ein ausgereiftes Gespür für die Risiken verfügen. Oftmals fehlt es nur an technischer Unterstützung oder einem konkreten Lösungsvorschlag.

Sie müssen auch beachten, wie die einzelnen Zielgruppen arbeiten. So können Sie IT-Profis sehr gut mit Live Hacking-Events sensibilisieren. Wirksam ist auch nachprüfbares richtlinienkonformes Verhalten mit dem Erreichen von Karrierezielen zu verbinden. Mitarbeiter im Risikomanagement haben z.B. oftmals einen akademischen Hintergrund und sind es gewohnt, lange Texte zu lesen und zu analysieren. Solchen Mitarbeitern können Sie Sicherheitsthemen mit fundierten Beiträgen und Hintergrundwissen vermitteln. Oberflächliche Präsentationen mit allgemeinen Aussagen sind bei Mitarbeitern mit Spezialkenntnissen in bestimmten Fachthemen eher schädlich.

Als Datenschutzbeauftragter müssen Sie die richtige Ansprache für die jeweiligen kritischen Zielgruppen in Ihrem Unternehmen finden. Das erreichen Sie nicht mit einer Awareness-Kampagne. Bei Fachspezialisten müssen Sie von einer ausgeprägten Kompetenz in Sicherheitsfragen ausgehen. Wenn Sie solche Fachspezialisten dazu verpflichten standardisierte WBTs zu absolvieren oder an Pflichtveranstaltungen zu Sicherheitsthemen teilzunehmen, werden Sie auf starke Gegenwehr stoßen. Sie müssen daher auf Kooperation setzen und mit den Menschen sprechen. Nur so können Sie vorprogrammierte Konflikte lösen und Ihre Ziele auch bei diesen Zielgruppen erreichen.

Fazit
Kooperation und Kommunikation auf Augenhöhe können Sie nicht verordnen. Die wenigsten Mitarbeiter haben solche kooperativen Arbeitsmodelle gelernt. Veranstalten Sie regelmäßige Treffen mit den jeweiligen Zielgruppen, bei denen Sie sich als Zuhörer und Berater präsentieren. Machen Sie aber deutlich, dass Sie genauso von den Erfahrungen und dem Wissen der Mitarbeiter profitieren wollen. So regen Sie zu einem lebendigen und kooperativen Wissenstransfer an, bei dem alle profitieren. Sollte sich dabei herausstellen, dass eine Ihrer Richtlinien nicht sinnvoll oder praktikabel ist, müssen Sie bereit sein, diese an die Erfordernisse der Zielgruppe anzupassen, sofern dies unter Risikogesichtspunkten vertretbar ist. Das wird dazu führen, dass Sie ernst genommen werden und man Ihre Meinung wertschätzt. Sie müssen die kooperative Zusammenarbeit vorleben, Zugeständnisse machen aber auch konsequent Maßnahmen einfordern.

Phishing-Mails mit Lucy. So erstellen Sie Ihre eigene Phishing-Mail.

Wenn Sie als Datenschutzbeauftragter kein ausreichendes Budget haben, um einen Phishing-Angriff mit Unterstützung externer Berater durchzuführen, können Sie einen solchen Angriff auch mit dem kostenlosen Tool Lucy durchführen. Sie sollten sich aber mit der IT-Abteilung abstimmen, denn Sie benötigen zur Installation administrative Berechtigungen und techn. Fachkenntnisse.

Vorbereitung. Diese Systeme benötigen Sie.
Sie benötigen zur Installation eine virtuelle Maschine mit einem Linux Betriebssystem. Das sollte Ihnen die IT-Abteilung auf einem eigenen Rechner mit Internetzugang installieren. Der Aufwand ist sehr begrenzt und die Installation sollte in einer Stunde fertiggestellt sein. Laden Sie danach die kostenfreie Version der Software Lucy herunter und installieren Sie diese auf Ihrem virtuellen „Server“.

Landing Page. So begrüßen Sie die Mitarbeiter.
Klicken die Mitarbeiter in der Phishing-Mail auf den präparierten Link, werden Sie auf eine Seite weitergeleitet auf welcher der eigentliche Angriff stattfindet. Diese sogenannte Landing Page können Sie in Lucy einfach aus einer großen Anzahl vordefinierter Seiten auswählen. Lucy kann sogar Ihre Internetseiten nachbilden. Für die

ersten Schritte reicht es aus, ein Template auszuwählen. Diese Templates enthalten bereits Eingabefelder für Benutzernamen und Passwort. Sie können auch verschiedene Szenarien wie z.B. Umstellung auf verschlüsselte E-Mails, Gesundheitstage usw. auswählen. Wählen Sie ein Szenario, das zu Ihrem Unternehmen passt, denn nur so können Sie die Mitarbeiter auch erfolgreich ködern.

Damit Sie Ihre Mitarbeiter auch in einem realistischen Szenario begrüßen können, sollten Sie für Ihre Landing Page eine eigene Domäne registrieren. Diese können Sie kostengünstig bei vielen Web-Hostern im Internet einrichten. Wählen Sie einen Domänennamen, der leicht mit der Domäne Ihres Unternehmens verwechselt werden kann. Wie z.B. „musterman.de“ anstelle von „mustermann.de“.

Phishing-Mail. So erstellen Sie die Vorlage.
Dank des integrierten E-Mail-Servers, können Sie direkt E-Mails mit gefälschten Absenderadressen versenden. So können Sie z.B. auch E-Mails im Namen Ihres Geschäftsführers versenden. Lucy bietet umfangreiche Möglichkeiten den Text zu formatieren. Sie können sogar mit Variablen arbeiten, die den Namen des jeweiligen Adressaten in die Textpassagen einbinden. So können Sie z.B. die E-Mails mit Anreden wie „Sehr geehrte Frau Mustermann“ personalisieren. Die Adressdaten lassen sich per Textdatei importieren. Haben Sie die E-Mailvorlage erstellt, kann es losgehen.

Trojaner. Diese Angriffe sind mit Lucy möglich.
Sie können mit Lucy auch Trojaner erstellen, die an die Mails angehängt werden. Den Trojaner konfigurieren Sie in Lucy mit wenigen Mausklicks. Sie können z.B. den Trojaner so konfigurieren, dass die letzten Dokumente des jeweiligen Opfers an eine festgelegte Adresse hochgeladen werden. Als Datenschutzbeauftragter müssen Sie beim Einsatz solcher Techniken aber zwingend Ihre IT-Abteilung informieren und das Vorgehen abstimmen. Auch die Geschäftsleitung und der Betriebsrat muss von Ihnen informiert werden.

Auswertung. Diese Informationen liefert Lucy.
Mit Lucy können Sie Ihre Phishing-Attacke sehr genau auswerten. Sie erhalten aussagekräftige Diagramme mit denen Sie auch Ihrer Geschäftsleitung darstellen können, wie der Angriff verlaufen ist. Als Datenschutzbeauftragter müssen Sie sich aber auch damit auseinandersetzen, dass Lucy jeden Klick und die Eingaben der Mitarbeiter aufzeichnet. Wenn Sie Benutzernamen und Passwörter abfragen, stehen diese Informationen später im Klartext auf Ihrem Server. Diese Daten müssen streng vertraulich behandelt und datenschutzkonform gelöscht werden.

Fazit
Mit Lucy können Sie sehr effektive Phishing und Social Engineering-Angriffe durchführen. Sie können sogar eigene Trojaner entwickeln. Damit haben Sie die Möglichkeit, die Wirksamkeit Ihrer Sensibilisierungsmaßnahmen zu messen und die Mitarbeiter gleichzeitig wachzurütteln. Aber schießen Sie nicht über das Ziel hinaus. Sie müssen darauf achten, dass Sie die Mitarbeiter nicht zu oft mit solchen Angriffen belasten. Das führt nämlich zu Gewöhnungseffekten und Widerständen. Am Ende erreichen Sie noch, dass echte Phishing-Mails oder Angriffe nicht mehr ernst genommen werden, weil jeder denkt, dass der Datenschutzbeauftragte wieder eine seiner „bekloppten“ Test-E-Mails verschickt hat.

Rubber Ducky. Führen Sie einen Angriff mit einem USB-Stick durch.

Mit Schadcode präparierte USB-Sticks werden sehr oft dazu genutzt, um Angriffe auf Unternehmensdaten durchzuführen. Aus diesem Grund haben sicherheitsbewusste Unternehmen in der Regel USB-Schnittstellen an den Rechnern gesperrt. Dieses Problem haben findige Hacker erkannt und Werkzeuge entwickelt, die es ihnen ermöglichen, trotz gesperrtem USB-Port, Angriffe über diese Schnittstelle durchzuführen. Ein solches Werkzeug ist der Rubber Ducky. Dieses Gerät sieht aus wie ein USB-Stick, ist aber in Wirklichkeit ein kleiner Computer, der sich am USB-Port eines Rechners als Tastatur ausgibt und in der Lage ist, vorprogrammierte Tastaturbefehle an den Rechner zu senden. Da viele Tastaturen an USB-Ports angeschlossen werden müssen, sind diese auch nicht gesperrt.

Vorbereitung. Das müssen Sie wissen.
Die Hardware können Sie im Internet bestellen. Die DeLuxe Ausführung kostet in einem Hacker Shop 44$. Das Gerät besteht im Wesentlichen aus einer auf 60 MHz getaktete CPU, einem microSD- Reader und einer passenden Speicherkarte. Auf der SD-Karte werden die Tastaturbefehle gespeichert, die der Stick beim Einstecken in

den Rechner automatisch ausführt. Eine Anleitung, wie Sie die Tasturbefehle auf der Speicherkarte ablegen können, finden Sie im Internet. Im Internet finden Sie auch ein Toolkit, das es Ihnen ermöglicht, auf einfache Art Scripte zu erstellen und diese in ausführbaren Code zu verwandeln.

Hallo Welt. So erstellen Sie Ihr erstes Script.
Wenn Sie das Toolkit heruntergeladen und gestartet haben, können Sie in einem Eingabefenster die einzelnen Befehle für Ihren Schadcode eingeben. Die Skriptsprache ist sehr einfach und trägt den Namen Ducky Script. Das Script besteht aus einer Textdatei, die eine Aneinanderreihung von Tastaturbefehlen und Pausen enthält. Ein erstes „Hello World“ sieht so aus:

```
DELAY 3000
GUI r
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 750
STRING Hello World!!!
ENTER
```

DELAY sorgt für eine einmalige Pause. Beide Zeitwerte gibt man in Millisekunden an. GUI steht für die Windows-Taste, GUI r für Ausführen. Mit STRING tippt der Stick ganze Zeichenfolgen ein. Dabei kümmert er sich automatisch um die Groß-/Kleinschreibung und eventuell vorhandene Sonderzeichen.

Schadcode. So bereiten Sie Ihren Angriff vor.
Obwohl die Scriptsprache sehr einfach ist, benötigen Sie sehr fundierte Kenntnisse über die Windows-Befehle die Sie für Ihren Angriff nutzen wollen. Schließlich können Sie in Ihren Scripten nur die Befehlsfolgen verwenden, wie sie mit der Tastatur eingegeben werden. Das wird schnell sehr komplex. Für Ihren Angriff sollten Sie daher auf vorgefertigte Scripte zurückgreifen. Sie finden im Internet eine Vielzahl von Beispielscripten, die Sie direkt verwenden können. Für Ihre erste Live Hacking-Vorführung sollten Sie mit einem einfachen Script starten. Nachfolgendes Script minimiert alle Fenster, macht einen Screenshot, öffnet Paint, kopiert den Screenshot in Paint und speichert ihn im Userprofil als Hintergrundbild ab.

```
GUI d
DELAY 500
PRINTSCREEN
DELAY 100
MENU
DELAY 300
STRING V
DELAY 40
STRING D
DELAY 300
GUI r
DELAY 700
STRING mspaint
ENTER
DELAY 1200
CTRL v
DELAY 500
CTRL s
DELAY 1000
STRING %userprofile%\a.bmp
```

```
ENTER
DELAY 500
ALT f
DELAY 400
STRING K
DELAY 100
STRING F
DELAY 1000
ALT F4
DELAY 300
GUI d
```

Kopieren Sie dieses Script in das Toolkit, kompilieren Sie das Script und speichern es auf der SD Karte. Legen Sie die SD-Karte in den Rubber Ducky.

Mein Tipp
Testen Sie das Script an dem Rechner, den Sie für Ihre Präsentation verwenden. Von zentraler Bedeutung sind die DELAY Zeiten im Script. Sind diese zu kurz, werden die Tastaturbefehle zu schnell an den Rechner übertragen und überlagern sich. Dadurch können sie vom Rechner nicht mehr ordnungsgemäß ausgeführt werden. Wählen Sie für Ihre Präsentation ruhig längere Zeiten aus, dann können die Zuschauer der Vorführung besser folgen.

Live Hack. Das sollten Sie beachten.
Wenn Sie das Script mehrmals erfolgreich getestet haben, können Sie Ihren Auftritt starten. Zeigen Sie den Zuschauern zunächst den Stick und erläutern Sie, dass auf dem Rechner USB-Sticks gesperrt sind. Erklären Sie kurz was die Zuschauer erwartet und stecken den Stick an den USB-Port. Sie werden sehen, dass Sie anschließend die volle Aufmerksamkeit der Zuschauer haben. Sie sollten nun kurz erklären, wie einfach dieser Angriff vorbereitet werden kann. Erläutern Sie anhand von Beispielen welche Scripte im Internet zur Verfügung stehen und was man mit diesen Scripten alles machen kann. Sie finden im Internet Scripte mit denen Sie Dateien aus dem Internet laden und starten können, Scripte mit denen Sie Dateien vom Rechner ins Internet hochladen können, Scripte, mit denen vollständige Shell-Scripte (VBS-Dateien) auf dem Rechner erstellt und ausgeführt werden und Scripte die Passwortattacken auf dem Rechner ausführen. Der Fantasie sind keine Grenzen gesetzt.

Fazit
Mit diesem Live Hack können Sie den Mitarbeitern zeigen, wie einfach es ist vorhandene Sicherheitsmaßnahmen zu umgehen und Angriffe auszuführen. Das kann jedermann ohne spezielle Kenntnisse. Es gibt für diese Angriffe auch techn. Schutzmaßnahmen. Diese sind jedoch in den wenigsten Unternehmen installiert. Es kommt also wie immer auf die Aufmerksamkeit der Mitarbeiter an. Diese müssen verhindern, dass Betriebsfremde oder auch Kollegen USB-Sticks an Rechner einstecken. Das müssen Sie in Ihrer Präsentation hervorheben.

Passwort-Hack. So knacken Sie Windowspasswörter.

Es gibt viele Möglichkeiten Windows-Passwörter zu hacken. Die meisten sind jedoch mit einigem Vorbereitungsaufwand verbunden und zielen eher auf die Passwortqualität ab. Es gibt aber auch einfache Verfahren, die gerade aus diesem Grund bei den Zuschauern für Verblüffung sorgen. Voraussetzung ist ein Windowsrechner mit Windows 7 bei dem eine lokale Anmeldung möglich ist. Der Rechner muss zudem über ein externes Speichermedium (CD, USB) starten können.

Vorbereitung. Diese Utensilien benötigen Sie.
Wenn in Ihrem Unternehmen Rechner mit DVD-Laufwerken eingesetzt werden müssen Sie vor der Präsentation prüfen, ob Sie beim Bootvorgang die Möglichkeit haben, das Startmedium (Festplatte, DVD, USB) auszuwählen. Das entsprechende Menü wird meist mit den Tasten „Entfernen“, bei einigen Computern aber auch mit „F2“, „F10“ oder den Tasten „Strg“ oder „Escape“ geladen. Wenn Sie einen externen Datenträger auswählen können, benötigen Sie für den Hack nur noch eine bootfähiges Speichermedium (USB, DVD) mit Windows. Sollten Sie den Rechner nicht über ein externes Speichermedium starten können, lesen Sie den Tipp am Ende des Artikels.

Durchführung. So gehen Sie konkret vor.
Um ein lokal gespeichertes Passwort zu hacken, müssen Sie den Rechner mit der CD booten. Nach der Auswahl der Sprache wählen Sie die Schaltfläche „Computerreparaturoptionen“. Je nach Setup- Medium kommen Sie dann entweder sofort zur „Eingabeaufforderung“ oder über die Klickfolge „Problembehandlung -> Erweiterte Optionen -> Eingabeaufforderung“. In der Eingabeaufforderung wechseln Sie mit „cd windows\system32“ in den Ordner mit den Systemprogrammen. Benennen Sie mit dem Befehl „ren utilman.exe utilman.ex_“ die Datei „utilman.exe“ um und kopieren dann die Eingabeaufforderung (cmd.exe) auf die Datei „utilman.exe“. Mit diesem Befehl „copy cmd.exe utilman.exe“ lösen Sie den Kopiervorgang aus.

Danach können Sie das System herunterfahren, die DVD entnehmen und den Rechner normal starten. Utilman.exe ist ein kleines Hilfsprogramm für Sehbehinderte („Erleichterte Bedienung“), das direkt am Anmeldebildschirm von Windows startklar ist. Wenn Sie nun im Anmeldebildschirm auf das Symbol „Erleichterte Bedienung“ klicken oder die Tastenkombination „Win-U“ betätigen startet nicht die Datei „utilman.exe“ sondern die Eingabeaufforderung „cmd.exe“. Jetzt müssen Sie nur noch den Befehl „net user konto kennwort“ eingeben. Wollen Sie z.B. das Passwort des lokalen Administrators hacken, geben Sie den Befehl „net user Administrator 123“ ein. Dieser Befehl ist direkt wirksam. Sie können sich unmittelbar als lokaler Administrator mit dem Passwort „123“ anmelden.

Denken Sie daran nach Ihrer Präsentation die Dateien wieder in Ihren ursprünglichen Zustand zu bringen.

Mein Tipp
Falls der Rechner kein CD-Laufwerk hat, können Sie auch die harte Tour fahren. Sie benötigen dann einen Rechner mit einem installierten Linux-System. Bauen Sie die Festplatte des Zielrechners aus. Das ist meistens ohne Werkzeug möglich. Schließen Sie die Festplatte an den Linux Rechner an und führen dort im Dateimanager die Umbenennung und den Kopiervorgang durch. Anschließend bauen Sie die Festplatte wieder in den Zielrechner und starten wie oben beschrieben. Je nach Zielgruppe ist dieses Vorgehen sogar zielführender als die CD-Variante. CD-Laufwerke und Bootoptionen lassen sich sperren, der Ausbau einer Festplatte kann nach Betriebsende von jedem Angreifer durchgeführt werden.