Bundesministerium
des Innern

SICHER GEWINNT
BAköV · BSI
SICHER GEWINNT

Sicher gewinnt!

Sensibilisierungsinitiative für Informationssicherheit in der Bundesverwaltung

Die Initiative – Resümee und Ausblick

BAköV

Sicher gewinnt!

Sensibilisierungsinitiative für Informationssicherheit
in der Bundesverwaltung

Die Initiative – Resümee und Ausblick

Bundesakademie für öffentliche Verwaltung
www.bakoev.de

Inhaltsverzeichnis

Vorwort

Das vorliegende Heft ergänzt die Reihe der Publikationen rund um unsere Informationsinitiative „Sicher gewinnt! – Informationssicherheit am Arbeitsplatz“ (Teil I – Leitfaden, Teil II – Werkzeugkasten). In diesem Heft kommen die Menschen zu Wort, mit deren Hilfe die Kampagne umgesetzt wurde. Sie berichten von ihren Erfahrungen aus Schulungen und Veranstaltungen oder geben einen kurzen Abriss darüber, wie die Kampagne in ihrer Behörde umgesetzt worden ist.

Sie finden hier Berichte und Lösungsansätze der Viefalt der Bundesverwaltung entsprechend. Eingeleitet wird dieses Kompendium mit Vorworten der Staatssekretärin im Bundesministerium des Innern und Beauftragte der Bundesregierung für Informationstechnik, Cornelia Rogall-Grothe, sowie der Präsidenten des Bundesamts für Sicherheit in der Informationstechnik, Michael Hange, und der Bundesakademie für öffentliche Verwaltung, Günther Wurster.

Auch die Teilnehmerinnen und Teilnehmer an den Seminaren und Veranstaltungen kommen in diesem Heft zu Wort. Und wir freuen uns, dass sowohl die Kampagne selbst, als auch die Umsetzung der einzelnen Maßnahmen so gut bei den Adressaten angekommen sind.

Das ist für uns die größte Motivation, die Sensibilisierung zur Informationssicherheit fortzusetzen.

Cornelia Rogall-Grothe
IT-Beauftragte der Bundesregierung

Angreifer machen keine Pause

Mit Beschluss des Deutschen Bundestags zum „Gesetz zur Sicherung von Beschäftigung und Stabilität in Deutschland“ wurde Anfang 2009 auch das IT-Investitionsprogramm auf den Weg gebracht: Damit sind insgesamt 500 Mio. Euro für Investitionen in Informations- und Kommunikationstechnik (IKT) zur Verfügung gestellt worden. Das IT-Investitionsprogramm zielt darauf ab, die Bundesverwaltung sicherer, umweltfreundlicher und bürgernäher zu gestalten und die deutsche IKT-Wirtschaft nachhaltig zu stärken. Es konzentriert sich auf die vier Maßnahmenbereiche: die IT-Sicherheit, die Verbesserung der IT-Organisation des Bundes, Green-IT und Zukunftsfähigkeit/Innovationen.

Mit der Sicherheit und Verfügbarkeit von IKT steht und fällt die Funktionsfähigkeit unserer global vernetzten Gesellschaft. Mit rund 230 Mio. Euro bildet „IT-Sicherheit“ den Schwerpunkt des Programms. Zu den 135 Maßnahmen zählen die Entwicklung und Beschaffung von Krypto-Handys und sicheren PDAs, die Verbesserung der Internetsicherheit und zentraler Einkauf von Produkten zur Abwehr von Schadprogrammen, der Ausbau der Sicherheit und Infrastruktur von Netzen der Bundeswehr, die Beschaffung von Kartenlesern inklusive Sicherheitssoftware für den neuen Personalausweis sowie flächendeckende IT-Sicherheitsberatung und -schulungen innerhalb der Bundesverwaltung. Ziel des IT-Investitionsprogramms ist auch, die Netze des Bundes noch effektiver gegen Ausfall und Angriffe von außen zu schützen und jederzeit eine mobile und sichere Kommunikation per Sprache, E-Mail oder Netzwerkzugriff sicher zu stellen.

Die BAköV hat in Zusammenarbeit mit dem BSI mit Mitteln des IT-Investitionsprogramms in bemerkenswerter Schnelligkeit eine Initiative zur Sensibilisierung aller Bundesbediensteten aufgestellt und durchgeführt. Das hohe Interesse ist ein Indiz, dass die Sensibilisierung der Mitarbeiter ein zentraler Baustein der Informationssicherheit ist. Dies möchte ich durch ein mir zugetragenes Beispiel belegen: Eine neue Angriffswelle eines „Homebanking-Trojaners“ erkannte ein Mitarbeiter richtig und eskalierte zeitnah an den IT-Sicherheitsbeauftragten. Dem zuvor sensibilisierten Mitarbeiter ist es zu verdanken, dass eine Infizierung vermieden wurde. Von technischen Schutzmaßnahmen wurde das Schadprogramm zu diesem frühen Zeitpunkt nämlich noch nicht erkannt. Wir wissen trotzdem, dass wir im Bereich Sensibilisierung immer noch viel Arbeit vor uns haben. Daher ist es notwendig, die Sensibilisierungsinitiative stetig der Bedrohungslage anzupassen und weiterzuentwickeln sowie entsprechende Module und Rahmenverträge der Initiative auch zukünftig zu nutzen. Die Angreifer machen bekanntlich auch keine Pause.

Für weitere Projekte der Sensibilisierung und Schulung zur Informationssicherheit in der Bundesverwaltung wünsche ich viel Erfolg.

Michael Hange

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Der Mensch trägt eine hohe Verantwortung

Der Staat entwickelt sich zunehmend zum Anbieter vielfältiger elektronischer Dienstleistungen. Trotz aller funktionaler Anforderungen darf die IT-Sicherheit nicht vernachlässigt werden. Der Staat hat Vorbildfunktion und entsprechend stellt der Bürger, der den Behörden seine Daten anvertraut, hohe Erwartungen an sichere Verwaltungsdienstleistungen.

IT-Sicherheit hängt aber nicht nur von der Umsetzung technischer Maßnahmen ab. Insbesondere die Mitarbeiter in Behörden tragen eine hohe Verantwortung im Umgang mit Informationen und Daten. Mit dem Ziel, das IT-Sicherheitsniveau in der Bundesverwaltung dauerhaft zu verbessern, befasst sich das BSI auch mit der Sensibilisierung und Beratung der IT-Nutzer in Bundesbehörden.

Die Initiative „Sicher gewinnt!“ der BAköV haben wir daher gern unterstützt.

Günther Wurster

Präsident der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern

Sensibilisierung zur Informationssicherheit ist Bildungsaufgabe

Die Sensibilisierung für den verantwortungsvollen Umgang mit Informationen an jedem Arbeitsplatz soll eine Übereinstimmung des Sicherheitsgefühls mit der Sicherheitswirklichkeit herstellen. Der Mensch bleibt der Sicherheitsfaktor Nummer 1. Wir sehen es als Bildungsaufgabe an, den Wunsch nach Sicherheit zu unterstützen und zu befähigen, Risiken abzuwägen.

Im Rahmen der Sensibilisierungsinitiative „Sicher gewinnt!“ wurde in Zusammenarbeit mit dem BSI und den IT-Sicherheitsbeauftragten der Behörden eine beeindruckende Leistung vollbracht. Von dem Angebot der Anpassung von Maßnahmen an die Behördenkultur wurde rege Gebrauch gemacht; es wurden über 44.000 Bedienstete in 97 Behörden geschult.

Da die Informationstechniken und Gefährdungen stetig fortschreiten, müssen auch wir das Können, Wissen und Wollen aller Bediensteten in der Informationssicherheit weiter entwickeln. Dies werden wir erreichen, indem wir die Sensibilisierung auch zukünftig als Prozess weiter betreiben.

Ausgangssituation und Zielsetzung

1. Sicher gewinnt! – Was erreicht werden sollte

Monika Elschner, Direktorin bei der Bundesakademie für öffentliche Verwaltung (BAköV)

Im Rahmen des IT-Investitionsprogramms der Bundesregierung konnte die BAköV im Rahmen ihrer Aufgabenerfüllung Mittel zur Unterstützung von Sensibilisierungsinitiativen und Schulungen für Informationssicherheit in der Bundesverwaltung zur Verfügung stellen. Die Basis bildeten der IT-Grundschutz und die Standards des Bundesamtes für Sicherheit in der Informationstechnik sowie der BAköV-Leitfaden „Sicher gewinnt! – Sensibilisierungsinitiativen für Informationssicherheit in der Bundesverwaltung".

Rahmenverträge im Drei-Partner-Modell

Zur Planung und Durchführung in den Behörden stellte die BAköV seit dem ersten Quartal 2010 Rahmenverträge im Drei-Partner-Modell für die Durchführung von Schulungs- und Unterstützungsleistungen zum kostenfreien Abruf bereit. Zwei Firmen, die secunet Security Networks AG und ML Consulting Schulung,

> *„Ich habe sehr viel Neues erfahren. Sehr interessantes Seminar, nicht zuletzt, weil viele reale Beispiele gezeigt wurden!"*

Service & Support GmbH, stellten Dienstleistungen im Bereich der Beratung und Schulung zur Verfügung. Die Firmen haben mit der Abgabe ihres Angebotes selbst entschieden, welche Aufträge von Behörden in welchem Postleitzahlenbereich, ob von 0000-4000 oder alle weiteren, in ganz Deutschland sie übernehmen wollten.

Die gesamte Sensibilisierungskampagne „Sicher gewinnt!" gliedert sich dabei in zwei Schwerpunktprojekte:

Das Projekt 1 unterstützte die Behörden bei der Vorbereitung, Planung und Durchführung von vielfältigen Sensibilisierungsmaßnahmen.

> *„Tolle Praxistipps für z. B. das sichere Löschen und Wiederherstellen von Dateien, Verschlüsselungen etc."*

Neben übergreifenden Maßnahmen in den Häusern sind Veranstaltungen für Führungskräfte und z. B. Beschäftigte in der IT eingeschlossen. Insgesamt haben über 97 Behörden einen Bedarf von 1800 Personentagen zur Durchführung von Sensibilisierungsmaßnahmen und zur Realisierung von Veranstaltungen mit Führungskräften und IT-Fachleuten angemeldet und umgesetzt.

Das Projekt 2 ermöglichte die Durchführung von Seminaren „Sicherheit am Arbeitsplatz" für alle Bediensteten. Über 44.000 Bedienstete haben Seminare zur „Informationssicherheit am Arbeitsplatz" besucht und Kenntnisse über

- Informationsquellen zur Informationssicherheit,
- die sichere Passwortwahl,
- die Vertraulichkeit und Weitergabe von Informationen,
- den Umgang mit E-Mails und Anhängen,
- ein gesundes Maß an Aufmerksamkeit,
- Wege der Information über Sicherheitsvorfälle,
- sowie aktuelle Entwicklungen erworben.

Das Angebot der BAköV zielte darauf, dass jede Behörde der eigenen Kultur entsprechend den individuellen Weg der Sensibilisierung beschreitet. Diese Vorgehensweise der Bereit-

stellung zentraler Angebote, Maßnahmen und Mittel verbunden mit der individuellen Anpassung erwies sich für die Vielfalt der Behörden in der Bundesverwaltung als der richtige Weg. Besonders wirkungsvoll war hier die Unterstützung der Fortbildungsbeauftragten.

Vielfalt des Werkzeugkastens

Neben den Rahmenverträgen stellte und stellt die BAköV über den Werkzeugkasten den IT-Sicherheitsbeauftragten der Bundesverwaltung weitere geeignete Instrumente und Materialien zur Durchführung von Sensibilisierungsmaßnahmen zur Informationssicherheit zur Verfügung. Der Werkzeugkasten ist gefüllt und füllt sich weiter mit Plakaten, Filmen, Flyern, Vorträgen und Studien sowie Beispielen, die in den Behörden entwickelt bzw. angepasst wurden. Auch für interessierte Dienststellen der Landes- und Kommunalverwaltung besteht die Möglichkeit, auf Teile des Werkzeugkastens zuzugreifen.

„Der Werkzeugkasten stellt eine sehr sinnvolle Ergänzung der gesamten Kampagne dar. Die medialen Inhalte sind sehr hilfreich bei der Sensibilisierung der Beschäftigten.“

Das Seminarangebot „Informationssicherheit am Arbeitsplatz“ wird durch eine Online-Version in einer elektronischen Lernwelt, welche auf der Lernplattform der BAköV eingestellt ist, ergänzt und ermöglicht die Vorbereitung auf den Test zum „Bundes-Informationssicherheits-Schein“ (BISS). Sowohl das Seminar als auch die Lernwelt und der „Bundes-Informationssicherheits-Schein“ werden in den Behörden teilweise verpflichtend weiterhin genutzt, um unter anderem neue Kolleginnen und Kollegen zu sensibilisieren.

In den Veranstaltungen und Gesprächen mit Führungskräften, gefördert mit zusätzlichen Geldern durch den IT-Stab, wurde darüber gesprochen, dass es um die Aktivität derjenigen geht, die Verantwortung tragen, und deren Vorbildfunktion. Auch die Festlegung von Verantwortung und die Überwachung der Umsetzung von Maßnahmen kann der Weg zur weiteren Stärkung der Informationssicherheit sein und ist nicht delegierbar.

„Es wurden Dinge, die im Grunde bekannt sind, auf eine interessante Weise neu ins Bewusstsein gerufen.“

Zum Erfolg der Kampagne „Sicher gewinnt!“ haben in vielen Behörden die Live-Hacking-Demonstrationen beigetragen. Diese haben sich auch schnell herum gesprochen, so dass es an Interessierten nicht gefehlt hat. Ein kleines aber eindrucksvolles Beispiel haben wir erlebt: Der kurzfristigen Einladung zur behördenübergreifenden Hacking Live-Demonstration mit Filmaufnahme sind so viele gefolgt, dass wir auf jeden der 120 Plätze zwei Teilnehmende hätten setzen können.

Wir werden also weiterhin solche Veranstaltungen anbieten.

Hacker-Veranstaltung mit Markus Linnemann und Marian Jungbauer in einer Behörde.

Aus den Veranstaltungen

2. … und so leicht gehackt!

Markus Linnemann,
secunet Security Networks AG

„… sehen Sie etwas auf dem Display des Handys? Können Sie irgendeine Veränderung erkennen, vielleicht ein eingehender Anruf? Nein? Aber können Sie sich im Lautsprecher des Hackers hören, wenn Sie jetzt in der Nähe des Telefons reden?

Ja?

Tja, das liegt an dem Trojanischen Pferd für Handys. Sie merken davon nichts, aber ein Angreifer kann alles hören, was in der Umgebung des Handys gesprochen wird, Ihre SMS und E-Mails lesen und sehen, wo Sie sind. Finden Sie das gut?“.

Ich kann Ihnen sagen, bisher fand das keiner der Befragten gut, dem ich diese Frage während einer Live-Hacking-Veranstaltung gestellt habe. Ganz im Gegensatz zu einer Demonstration eines solchen Angriffs auf ein handelsübliches Smartphone. Faszinierte, teilweise auch geschockte Blicke finden sich im Publikum, wenn der Hacker Telefone belauscht, eine SMS liest, ganze Computer fernsteuert oder Passwörter live vor Ort knackt.

Aber keine Bange, es soll nicht einfach schockiert werden. Bei allen Angriffsarten wird erläutert, wie sich Anwenderinnen und Anwender verhalten müssen, um sich vor diesen Angriffen zu schützen.

Die Technik kann bereits in vielen Fällen vor Cyber-Attacken schützen, aber das Live-Hacking verdeutlicht, dass die Technik richtig genutzt werden muss, um die notwendige Informationssicherheit herzustellen.

„Die Veranstaltung hat das Interesse der Beschäftigten für IT-Sicherheit geweckt und gleichermaßen betroffen gemacht. Das Hacking ist daher die beste Werbung für ein eher unbeliebtes Thema.“

Gleichzeitig wird ein Verständnis für die technischen Maßnahmen geschaffen, da es vielen Anwendern schwer fällt, technische, meist einschränkende Maßnahmen zu verstehen oder zu unterstützen. Dazu gehört die Notwendigkeit, komplexe, lange Passwörter zu wählen oder USB-Sticks nur nach bestimmten Regeln einzusetzen. So wie der Rückgang schwerer Verletzungen bei Autounfällen für jeden das Anlegen des Gurtes verständlich macht, schafft das Live-Hacking Verständnis für Informationssicherheitsmaßnahmen.

„In unserem Haus kam die Hacker-Veranstaltung sehr gut an. Es fielen Begriffe wie Lebendigkeit, Praxisnähe und gutes Zusammenspiel der Dozenten (das Team Linnemann/Jungbauer kam sehr gut an).“

Das Erfolgsrezept ist einfach: Alle zu vermittelnden Themen werden live demonstriert. Die „Hacker“ vom Institut für Internet-Sicherheit und der secunet Security Networks AG führen zu zweit durch die Veranstaltung. In einer Art Rollenspiel werden die Themen mit viel Humor und Geschichten aus dem wahren Leben vorgetragen. Durch die gleichzeitige Darstellung der Anzeige des Hackers und des Opfers über zwei Projektionsflächen kann der Zuschauer immer direkt verfolgen, was passiert und Aktion und Reaktion in Beziehung setzen, selbst wenn der Hacker ganz „Informatiker-like“ Textbefehle in eine Konsole eintippt.

Das Live-Hacking erzielt vor allem:

1. das Verständnis, dass Informationssicherheit jeden betrifft.
2. die Erkenntnis, dass Informationssicherheit wichtig und nicht langweilig ist.

Mit einer Schulung ist das Live-Hacking also nicht zu vergleichen, es eignet sich vielmehr als Auftakt für eine Schulungsreihe und besonders zur Sensibilisierung von Führungskräften. Aber auch für die IT selber, beispielsweise Administratoren, kann das Live-Hacking sehr effektiv eingesetzt werden. Je nach Zielgruppe werden die Ansprache und die technische Tiefe angepasst.

Bewährt hat sich außerdem ein Mischkonzept: Eine Person führt durch die Veranstaltung und vermittelt themenspezifische Inhalte. Die Hacker unterstützen die jeweiligen Themenblöcke mit Live-Präsentationen. So werden zusätzlich Schulungsinhalte vermittelt – ideal für Führungskräfte.

Die alten Szenarien werden bald als Schulungsfilm angeboten. Neue Szenarien befinden sich in der Vorbereitung. Lassen Sie sich überraschen und lassen Sie sich (nicht) hacken...

Aus den Behörden

3. BMWI – mach mIT

Dr. Stefan Afting, IT-Sicherheitsbeauftragter des BMWi

Wer sich intensiv mit IT-Sicherheit beschäftigt weiß: Nichts ist sicher. Nun, ganz korrekt ist das nicht, denn eins ist schon sicher: ohne die Mittel und Unterstützung der Bundesakademie für öffentliche Verwaltung (BakövV) wäre die Kampagne „mach mIT – Für mehr IT-Sicherheit im BMWi“ nicht so schnell an den Start gekommen.

Nach der Zusage und Vertraggestaltung durch die BAköV konnte mit der Planung der Kampagne im März 2011 begonnen werden.

Eine Erfahrung vorweg: Eine Sensibilisierungskampagne zu planen und durchzuführen macht Spaß! Sie fordert Kreativität und neue Betrachtungsweisen, aber sie kostet auch viel Zeit. Auch, wenn der unterstützende Dienstleister – die Firma secunet – viele Erfahrungen und Ideen einbringen und viele Arbeiten übernehmen kann.

Die Basis einer guten Kampagne ist ein gutes Konzept. Hier hat das BMWi drei Personengruppen und Vorgehensweisen in den Mittelpunkt der Kampagne gestellt:

- Präsentationsveranstaltungen mit Live-Hacking für die Leitung
- Workshops zur IT-Sicherheit mit den Administratoren
- Ein Bündel an Maßnahmen für die Beschäftigten im BMWi

Das Bündel besteht vor allem aus einem neuen Intranetportal zur IT-Sicherheit im BMWi. Über das Portal sollen die Beschäftigten auch über die Kampagne hinaus zur IT-Sicherheit informiert werden. Um zum Besuch der Seite zu motivieren, wurden vielseitige Maßnahmen ergriffen, die auf unterschiedlichste Weise das Thema transportieren. Dazu gehören ein eigenes Logo, mehrere Plakate, Comics, Filmclips, Tablettunterlagen in der Mensa und Live-Hacking-Veranstaltungen. Alle Maßnahmen sind aufeinander abgestimmt.

Ein Film mit Staatssekretär Kapferer zum Start der Kampagne hat für die nötige Aufmerksamkeit im Haus gesorgt und den Stellenwert der Informationssicherheit im Haus klargestellt.

Inhaltlich werden in der Kampagne über 12 Monate sechs Hauptthemen adressiert:

- Mobiles Arbeiten
- Passwort
- Datenträger
- Soziale Netzwerke
- E-Mails und Dokumente
- Social Engineering

Jedes Hauptthema ist im Logo durch ein eigenes Icon repräsentiert und wird bei der Veröffentlichung im Intranetportal von Plakten und Aktionen begleitet.

Darüber hinaus wird die mediale Präsenz der Kampagne genutzt, um neue Prozesse und Lösungen zur IT-Sicherheit im BMWi einzuführen.

Begonnen hat die Kampagne im September 2011. Sie wird bis zum Sommer 2012 weitergeführt.

Aus den Behörden

4. Bundeskanzleramt – Fortsetzung folgt

Andreas Hollweck, IT-Sicherheitsmanagement des Bundeskanzleramtes

Während die Nutzer von Informationstechnik von klassischen Bedrohungen wie Einbruch und Feuer eine klare Vorstellung haben, sind die Bedrohungen der IT insbesondere für den Nicht-Fachmann sehr abstrakt und wenig greifbar. Damit erschließt sich die Sinnhaftigkeit der organisatorischen und technischen Absicherungsmaßnahmen oftmals nur schwer und führt in der Folge nicht selten zu Akzeptanzproblemen.

Die Aufgabe für das IT-Sicherheitsmanagement im Bundeskanzleramt bestand deshalb darin, durch Sichtbarmachen der Gefährdung alle Anwenderinnen und Anwender für die Informationssicherheit am Arbeitsplatz zu sensibilisieren und Motivation zum Mitmachen zu erzeugen. Ein durchdachtes und überzeugendes Konzept bot die Initiative „Sicher gewinnt“ der BAköV an. Sie stellte mehrere Pakete zur Verfügung, die es erlaubten, eine auf die Besonderheiten des Amtes zugeschnittene Kampagne zu projektieren und durchzuführen.

Nach ausführlichen Diskussionen – auch mit externen Fachleuten – fiel die Entscheidung für Workshops, mit denen alle Mitarbeiter/-innen direkt angesprochen werden sollten. Die unterschiedlichen Bedürfnisse wurden durch verschiedene Schwerpunkte und Präsentationsformen berücksichtigt. So wurden spezielle Workshops für die Führungsebene, für Nutzer mobiler IT und für Nutzer mit vielfältigen Aussenkontakten („Social Engineering“) angeboten.

Mangels eigener Ressourcen wurden die Workshops durch externe Spezialisten durchgeführt. Dabei war es für den Erfolg ganz entscheidend, die Workshops, die im Grundsatz vorgefertigt waren, in intensiven Vorgesprächen auf die Kultur und die Bedürfnisse unseres Hauses anzupassen. Zusätzlich nahmen, wann immer es ging, IT-Fachkräfte des Hauses teil, was ihnen ermöglichte, Inhalte nachzujustieren und Probleme der Nutzerinnen und Nutzer aufnehmen zu können.

Es zeigte sich, dass insbesondere praxisnahe Beispiele – auch aus dem privaten Umfeld – ein hohes Maß an Betroffenheit erzeugten. So äußerten sich viele Teilnehmenden überrascht über Art und Umfang der tatsächlichen Bedrohungen. Skeptiker konnten schließlich mit Berichten von realen Cyber-Angriffen auf das Bundeskanzleramt überzeugt werden.

Den Erfolg der Maßnahmen zeigt den deutlich angestiegenen Beratungsbedarf zu IT-Sicherheitsfragen und die spürbar verbesserte Akzeptanz von einschränkenden Maßnahmen im IT-Umfeld.

Nachdem die initiale Sensibilisierung zur Informationssicherheit ein Erfolg war, kommt es nunmehr darauf an, durch weitere Maßnahmen das Erreichte nachhaltig zu festigen.

Aus den Behörden

5. BKA – Ich denke mit

Dr. Peter Frodl, IT-Sicherheitsbeauftragter des Bundeskriminalamtes (BKA)

Das BKA verarbeitet als Zentralstelle der deutschen Polizei, als für die internationale Zusammenarbeit verantwortliche Behörde, als ermittelnde Behörde und im Rahmen seiner Schutzaufgaben personenbezogene und anderweitig sensible Informationen in vielfältiger Weise. Es trägt daher eine besondere Verantwortung für deren Schutz. Dieser Verantwortung kann nur gerecht werden, wenn alle Beschäftigten sich der Risiken im Umgang mit diesen Informationen, insbesondere bei der digitalen Informationsverarbeitung, bewusst sind. Zielgruppe der Sensibilisierungskampagne zur Informationssicherheit waren deshalb alle 5.500 Beschäftigten auf allen Ebenen und in allen Abteilungen des BKA. Die Kampagne wurde von der Amtsleitung und der Personalvertretung unterstützt.

Die Kampagne wurde mit einem eigenen Logo unter dem Motto „Ich denke mit! – Informationssicherheit im BKA“ entwickelt und durchgeführt. Dieses zur Amtskultur des BKA passende Motto sollte die Verantwortung jedes Einzelnen hervorheben.

Die Mitarbeiter des IT-Sicherheitsbeauftragten erarbeiteten die Inhalte des für alle Bediensteten obligatorischen Standardseminars „Informationssicherheit am Arbeitsplatz“ mit den Schwerpunkten „Mobile IT-Geräte“, „Speichermedien“, „Internet“ und „Social Engineering“. Die tägliche Praxis der Beratung von IT-Anwendern und -Betreibern sowie regelmäßige Gespräche mit IT-Fachkräften hatten gezeigt, dass bei diesen Themen noch häufig Unsicherheit bei den Anwendern vorherrscht, und dass Hinweise zum sicheren Umgang damit notwendig und auch willkommen sind.

Die Trainer von ML Consulting führten nach einem gemeinsamen Workshop mehr als 260 Schulungen durch. Passend zu den Themenschwerpunkten wurden Plakate entwickelt und über einen Zeitraum von acht Monaten im gesamten BKA publiziert. Weiterführende Informationen wurden im Intranet veröffentlicht. Ein selbstentwickeltes Online-Quiz mit Gewinnmöglichkeit (Tassen mit dem Kampagnenlogo) ergänzte den Intranetauftritt.

Für das IT-Personal wurde eine gesonderte Kampagne mit zielgruppenorientierten Workshops, Schulungen und Plakaten durchgeführt. Neben der Sensibilisierung stand hier die Vermittlung von fachspezifischem Wissen zum Thema Informationssicherheit im Mittelpunkt.

Zusätzlich zu den Sensibilisierungsschulungen konnten insgesamt ca. 1.000 Mitarbeiterinnen und Mitarbeiter in sechs Live-Hacking-Vorführungen ganz praktisch verfolgen, wie bei sorglosem Umgang mit Informations- und Kommunikationstechnik Sicherheitslücken von Unberechtigten ausgenutzt werden können.

Insgesamt haben alle Maßnahmen das Thema Informationssicherheit stärker in die Wahrnehmung gerückt und damit einen Lernprozess angestoßen, den wir nachhaltig begleiten wollen.

Aus den Behörden

6. Bundesfinanzdirektion SO – Interesse gesteigert

Norbert Neubauer, IT-Sicherheitsbeauftragter der Bundesfinanzdirektion Südost

Die Bundesfinanzdirektion Südost, einschließlich der Bundeskasse Weiden, hat von März 2010 bis April 2011 an der Sensibilisierungsinitiative „Sicher gewinnt“ zur Sensibilisierung und Schulung zur Informationssicherheit für alle Bundesbediensteten teilgenommen.

Die Einführungsveranstaltungen (Live-Hacking-Show) wurden sehr gut aufgenommen und haben das Interesse an den nachfolgenden Seminaren „Informationssicherheit am Arbeitsplatz“ (ISaA-Seminare) nachhaltig gesteigert. Gleichzeitig ist die IT-Sicherheitsleitlinie der Behörde vorgestellt und eingeführt worden.

Im Anschluss wurden vier spezifische Seminare für verschiedene Zielgruppen (IT-Administratoren, Führungskräfte, Zollzahlstellenprüfer) durchgeführt.

An den 26 ISaA-Seminaren haben insgesamt 237 Anwender/innen teilgenommen. Die Möglichkeit zum Erwerb des Bundes-Informationssicherheits-Scheins („BISS“) wurde ebenfalls von etlichen Anwender/innen wahrgenommen.

Diese Seminare wurden zeitnah evaluiert und der Gesamteindruck der Seminare wurde mit über 95 Prozent als gut oder sehr gut bewertet, die Veranstaltungen als „abwechslungsreich“ und „ansprechend“ eingestuft. Der zeitliche Umfang wurde mit 90 Prozent gut bewertet. Einzelne fanden drei Stunden für die vermittelten Inhalte zu lang; für Andere waren es zuviele Informationen in zu kurzer Zeit.

Inhaltlich waren die Seminarteilnehmer/innen der Meinung, dass dienstliche Belange wie z. B. dienstliche Internet- / E-Mailnutzung, Risiken von Internet und Sicherheitssoftware, Schwachstellen und Verbesserung der Sicherheit beim täglichen Umgang mit dem PC, Stand der IT-Sicherheit im Haus bzw. Bezirk der Dienststelle stärker hätten berücksichtigt werden sollen.

Im privaten Bereich waren insbesondere aktuelle Informationen zu Malware und zum neuen Personalausweis (Anwendungsmöglichkeiten und Gefahren) gefragt, sowie die Gefährdungen durch unscheinbare Gefahrenquellen, z.B. Drucker, Spielkonsole, USB-fähige Geräte.

Um erworbenes Wissen zu wiederholen oder aufzufrischen wurde zu den Seminaren auch der Einsatz von E-Learning-Angeboten oder anderen Schulungsangeboten angeregt. Darüber hinaus wurden über das Behörden-Intranet Filme, Texte und Bilder zum Thema angeboten.

Die durchgeführte Sensibilisierungsinitiative wird von uns als beachtlicher Erfolg bewertet, insbesondere weil die Sensibilisierungsinitiative von unserem Präsidenten nachhaltig unterstützt wurde. Einführungsveranstaltungen wurden von ihm oder seinem Vertreter persönlich eröffnet. Auch die mittlere Führungsebene hat Anwender/innen teilweise nachdrücklich zur Teilnahme an den Seminaren motiviert.

Aus den Behörden

7. PTB – Seminare und eTutorials

Dr. Hans-Georg Kerkhoff, IT-Sicherheitsbeauftragter der Physikalisch-Technische Bundesanstal

Die Physikalisch-Technische Bundesanstalt (PTB) ist das nationale Metrologie-Institut mit wissenschaftlich-technischen Dienstleistungsaufgaben. Unser Aufgabenspektrum reicht von der Grundlagenforschung mit geringeren Anforderungen bis zur Bearbeitung hoheitlicher Aufgaben mit hohen Anforderungen an die Informationssicherheit. Hoheitliche Aufgaben erfordern eine restriktive Herangehensweise; die BSI Vorgaben für den Grundschutz werden daher eng ausgelegt.

Die Herausforderung besteht für uns darin, die bei der PTB gewünschte und notwendige spontane Kommunikation zwischen Wissenschaftlern zu sichern und dabei trotzdem hohe Sicherheitsstandards einzuhalten. Unsere technischen Schutzmaßnahmen sind hierfür grundsätzlich ausreichend und sollen nur bei Bedarf erhöht werden.

Vor der Technik kommt der Mensch, vor allen Dingen in forschungsorientierten Einrichtungen, weswegen die PTB auf eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter setzt. Das Ziel: der sorgsame und bewusste Umgang mit der IT. Die Führungskräfte der PTB übernehmen dabei die Rolle von Multiplikatoren, haben also selbst eine Vorbildfunktion inne.

In den Auftaktveranstaltungen zu Beginn der Kampagne im Herbst 2010 wurde auf die Bedrohung der Datensicherheit von außen aufmerksam gemacht. Unterstützt durch praktische Beispiele, wurde allen Teilnehmenden vermittelt, dass sie selbst jederzeit Angriffen von außen ausgesetzt sein können.

In der ersten Jahreshälfte 2011 initiierte der IT-Sicherheitsbeauftragte regelmäßige Projekttreffen mit den Fachverantwortlichen für die IT-infrastrukturellen Dienstleistungen. Danach wurden konkrete Sicherheitsmaßnahmen entwickelt, Verantwortungen definiert, Lösungen umgesetzt und die Realisierung begleitet. Das Ergebnis sind 10 Themenschwerpunkte (u. a. verschlüsselte USB-Sticks, Signieren und Verschlüsseln von E-Mail (S/MIME) mit Zertifikaten aus der PTB CA), welche die Grundlage für die Workshops 2011 „Sekretariate“ und „Mitarbeiterinnen und Mitarbeiter mobiler Arbeitsplätze“ bildeten.

Sehr früh wurde deutlich, dass der Umfang dieser Themen nicht in zweistündigen Workshops vermittelt werden kann. Daher erstellte der IT-SiBe begleitende Schulungsunterlagen, die auch später, nach Abschluss der Kampagnenumsetzung, eigenständig als Hilfe verwendet werden können. Da diese Unterlagen im Intranet interaktiv zur Verfügung stehen, wurden sie eTutorials genannt.

Bei den „eTutorials“ handelt es sich um einfache „Computer Based Tutorials“ im PTB-Intranet. Die Fülle und die Komplexität der zehn Themen boten sich perfekt an, um interaktive Lerngruppen im Intranet zur Verfügung zu stellen. In den Workshops , die in Phase III der Kampagnenumsetzung stattgefunden haben, wurde bei der Erläuterung von Lösungen auf die eTutorials verwiesen.

Die Ergebnisse zeigen, dass wir im Herbst 2011 zwar die Kampagne beenden; das Thema wird jedoch noch weiter präsent bleiben.

Aus den Behörden

8. BIBB – Siggi, unser neuer Freund

Dr. Astrid Fey, IT-Sicherheitsmanagement des Bundesinstituts für Berufsbildung

Das Gesicht der Kampagne „Sicher gewinnt!“, Siggi Sicher, ein kleiner, sympathischer Helfer in allen Fragen und Nöten der IT-Sicherheit, hat mit seiner freundlichen Art schnell die Herzen im Bundesinstitut für Berufsbildung (BIBB) gewonnen.

Bundesinstitut für Berufsbildung

BIBB

Forschen
Beraten
Zukunft gestalten

Der „große Siggi“, er mag den Vergleich mit einem Aufsteller aus Pappe und Stahl gar nicht, hat die Kampagne von Anbeginn begleitet. Er „arbeitete“ zeitweise im Foyer und begrüßte gleichermaßen Beschäftigte und Gäste. Ebenso schaute er in diversen Sitzungssälen, in denen alle Mitarbeiterinnen und Mitarbeiter in halbtägigen Schulungen ihr Wissen über die IT-Sicherheit erweiterten, vorbei. Heute, nach Abschluss der Kampagne „wohnt“ er im Büro der IT-Referatsleiterin und nimmt rege Anteil, beispielsweise an Besprechungen. Kidnapping-Versuche konnten bisher erfolgreich abgewehrt werden.

Mit der Teilnahme an der Sensibilisierungskampagne erhielten alle Beschäftigte des BIBB einen „kleinen Siggi“. Diese sind sehr anhänglich – oberflächlich könnte man sie als Aufkleber bezeichnen – und kleben vielfach an den Arbeitsplätzen.

Der Star unter den Siggis ist zweifellos der kleine Mann aus Gummimasse. Man kann ihn knautschen, herzen, auf die Kasse der Kantine kleben – er macht alles mit. Er fällt um und steht wieder auf.

Im Bundesinstitut wurde im Verlauf der Kampagne mit der Institutsleitung und dem Personalrat Einvernehmen darüber erzielt, dass die Teilnahme am Erwerb des BISS, dem Bundes-Informationssicherheits-Schein, für jede/n Beschäftigte/n des BIBB obligatorisch ist. Dies haben wir nunmehr in einer Institutsanweisung eigens festgeschrieben. Ist der BISS geschafft, winkt als Anerkennung eine Urkunde, aber vor allem ein „eigener“ Siggi.

Nach unserer Kenntnis hat Siggi so viel zu tun, dass er bisher keine Frau gefunden hat. Wir würden uns freuen, wenn wir die BAköV hierbei unterstützen könnten und damit der Nachwuchs in der Familie Sicher gesichert wäre.

Im Bundesinstitut zumindest sind alle Mitglieder jederzeit herzlich willkommen. Es wurde viel Gutes mit der Kampagne erreicht, das Resümee ist uneingeschränkt positiv ausgefallen. Allerdings gibt es in der IT-Sicherheit weiter viel zu tun, die Angreifer werden nicht müde, immer neue Bedrohungslagen zu schaffen.

Siggi – weiter so!

Ein Trainer berichtet

9. Unterwegs im Namen der Informationssicherheit

Severin Rast, mit Siggi Sicher

Ein Bereitschaftsraum im Keller eines Zollamtes an einem Hauptbahnhof mitten in Deutschland. An den zusammengeschobenen Tischen vor der kleinen Küchenzeile sitzen knapp fünfzehn gestandene Zöllner mit verschränkten Armen und beobachten kritisch den im Schnitt zehn Jahre jüngeren Dozenten der vorne mit Notebook und Beamer über Viren, Passwörter und Social Engineering spricht.

Der Dozent war ich, und nach einem knappen halben Jahr Schulungen hatte ich zum ersten Mal in der Kampagne das Gefühl, eine Gruppe überhaupt nicht zu erreichen. Alle Versuche, diesen Teilnehmern persönliche Erfahrungen oder Meinungen zu entlocken, wurden bestenfalls mit einem Brummen oder Nicken quittiert. Als der IT-Sicherheitsbeauftragte nach der Veranstaltung auf mich zukommt, rechne ich mit dem Schlimmsten.

"*Gefällt mir. Die haben doch gut mitgemacht!*" – Das war der letzte Satz, den ich erwartet hätte.

Aber auch nach Auswertung der Bewertungsbögen war klar, die Teilnehmer fanden die Themen interessant und die Veranstaltung gelungen. Über 15 Monate bin ich jetzt in ganz Deutschland im Namen der Informationssicherheit unterwegs und egal wohin es mich verschlagen hat, überall waren die Menschen die Herausforderung.

„Der Dozent berichtete lebhaft und damit besonders einprägsam über die Gefahren für die Informationssicherheit aufgrund des Faktors Mensch".

„... hatte viel Spaß beim Zuhören!"

„... selten so gelacht. Der Dozent hat die Probleme lebensnah dargestellt. Arbeitsklima war super. Dozent war spontan und flexibel."

„Der Dozent hat ein sehr ganzheitliches Verständnis von IT-Sicherheit vermittelt."

Die Technik ist im Großen und Ganzen immer die Gleiche und die Themen sind es ebenso. Die Menschen jedoch sind immer wieder für Überraschungen gut.

Die einen lehnen sich eben zurück und die Beschäftigung findet hinter ihren buschigen Augenbrauen statt, die anderen wollen ihre eigenen Geschichten loswerden und warten nur darauf, dass der Dozent mal die Klappe hält. In den weit verstreuten Dienststellen der Bundesanstalt Technisches Hilfswerk (THW) freute man sich über den Besuch aus dem fernen Köln und diskutierte die Schwierigkeiten bei der Kommunikation mit den vielen Ehrenamtlichen. Dazu gab es Kaffee und Kuchen – und beim Landesverband Sachsen Thüringen sogar ein Räuchermännchen im THW-Look! Den Webredakteuren einer Bonner Behörde brannte das Thema Facebook-"Gefällt mir"-Button und Datenschutz unter den Nägeln und andernorts wurde die Frage der "fortgeschrittenen" oder "qualifizierten" elektronischen Signatur heiß diskutiert.

„Mitgenommen habe ich tatsächlich eine sensiblere Haltung zu meinen Daten im Internet. Ich habe z. B. mehrere Accounts gelöscht, die ich nicht mehr brauche, mein Profil bei wer-kennt-wen *komplett minimiert und den Bundes-Informationssicherheits-Schein erworben.*

Nur die html-Ansicht in Outlook habe ich noch nicht geändert. Zu sehr liebe ich die Smilys und die schöne Schrift mit Absätzen und und und …"

Computer, Internet und Smart-Phones haben innerhalb kürzester Zeit unseren Alltag erobert, wir nutzen sie inzwischen dienstlich genauso wie privat und sind dabei oft rund um die Uhr online. Der sicherheitsbewusste Umgang mit den neuen Medien und Techniken stand bei dieser rasanten Entwicklung in den letzten Jahren oft hintenan. Und wenn nicht, dann waren es meist einige wenige System-Administratoren, die den Kolleginnen und Kollegen ihr technisches Sicherheitskonzept vorgesetzt haben.

Mit der Kampagne "Sicher gewinnt" haben wir nicht nur das Sicherheitsbewusstsein der IT-Nutzer/innen geweckt und gefördert, sondern auch ihr Selbstbewusstsein im Umgang mit der Technik. Und das ist die beste Vorraussetzung für Interesse, Engagement und Wachsamkeit.

Evaluierung – aber richtig

10. Wie messen wir Rückmeldungen ?

Matthias Kessler, secunet Security Networks AG und Gerd-Jürgen Peter, ML Consulting GmbH

Warum Evaluation?

Informationssicherheit ist ein permanenter Prozess und erfordert dauerhaft zielgenaue Maßnahmen, die ständig an sich ändernde Rahmenbedingungen angepasst werden müssen, um die Aufmerksamkeit für das Thema zu erhalten. Dies bedeutet, dass getroffene Maßnahmen hinsichtlich ihrer Wirksamkeit und Aktualität untersucht werden müssen und dieses Feedback in weiterführende Aktivitäten und deren Optimierung einfließt. Bereits bei der Definition der Ziele einer Sensibilisierungskampagne muss deren Evaluation vorbereitet werden.

Was woll(t)en wir wissen?

Ist eine Sensibilisierung für Informationssicherheit in der Behörde erreicht worden? Wie füllen Führungskräfte ihre Vorbildfunktion aus? Ist die Akzeptanz für Maßnahmen zur IT-Sicherheit gewachsen? Hat die Aufmerksamkeit an jedem Arbeitsplatz zugenommen? Verbessern Führungskräfte ihre Vorbildfunktion hinsichtlich der Informationssicherheit? Stellen Administratoren eine geänderte Aufmerksamkeit zu diesem Thema fest? Haben die Mitarbeiter/innen ihre Verhaltensweise in bestimmten Situationen geändert? Was ist nachhaltig im Bewusstsein der Mitarbeiter geblieben?

Wie sind wir vorgegangen?

Hierzu wurden in unterschiedlichen Behörden verschiedene Methoden eingesetzt, oft auch in Kombination:

- Auswertung mit Fragebögen, die auf die Ergebnisse zu den Zielen der jeweiligen Maßnahme und auf das Thema Verhaltens-/ Bewusstseinsveränderungen eingehen
- Auswertung der Anfragen an die IT-Hotline der Behörde - eine Methode, die klare Vorgaben zur Beurteilung der Ergebnisse erfordert. Hierzu müssen Parameter wie z. B. Inhalt der Anfragen untersucht werden
- Interviews, eine ressourcenintensive Methode, die deshalb nur stichprobenhaft angewendet wurde
- Anzahl der erfolgreichen Absolventen des Bundes-Informations-Sicherheits-Schein (BISS)
- Auswertung von Intranetaktionen, z. B. Quiz, Lückentexte, unvollendete Meldungen

Ein indirekter Indikator zur Evaluierung ist der Grad des Interesses für das Thema Informationssicherheit. Beispielweise wurde in einer Behörde ein Wettbewerb zur Namensgebung der behördeninternen Symbolfigur durchgeführt, mit großer Resonanz, ebenso fanden Postkarten mit goldenen Regeln einen hohen Absatz. Auch lassen sich Klicks auf die Intranetseiten zum Thema Informationssicherheit auswerten.

Foto: Berater und Sicherheitsbeauftragter analysieren den Fragebogen

Welche Ergebnisse brachte die Auswertung der Evaluation bisher?

Der Bekanntheitsgrad des Sicherheitsmanagements, dessen Aufgaben und Verantwortlichkeiten sowie der entsprechenden Vorgaben hat sich deutlich erhöht. Meldewege bzw. eine Orientierung für das, was im Notfall zu tun ist, waren z. T. vorher fast unbekannt. Dieser positive Effekt trat hauptsächlich dort ein, wo die Sicherheitsbeauftragten bei Schulungen dabei waren bzw. die entsprechenden Regelungen in Auszügen in den Vortrag integriert wurden. Generell erwiesen sich die Sensibilisierungsschulungen auch als Diskussionsplattform.

Ein weiterer Punkt war die Sensibilisierung für die Gefahren, die in den Social Networks lauern. Hilfestellungen zum Umgang mit der Passwortproblematik, konkrete Handlungsvorschläge zur sicheren Nutzung des Internets oder von USB-Medien waren ebenfalls ein häufig genannter Nutzen.

Nicht unerwähnt bleiben soll auch der Aufbau einer gewissen „Kontrollfunktion“ innerhalb der Mitarbeiter. Man macht sich gegenseitig auf Versäumnisse aufmerksam und ermuntert dazu, die Aufmerksamkeit hochzuhalten. Es konnte beobachtet werden, dass eine deutlich höhere Sensibilisierung für Gefahren und Risiken erfolgt ist. Dafür haben insbesondere die Hackervorführungen gesorgt.

Entscheidenden Einfluss auf die eingetretenen Veränderungen hatte dabei das Seminar „Informationssicherheit am Arbeitsplatz“. In den Feedbacks kam deutlich heraus, dass auch da, wo nicht alle Mitarbeiter, z. b. über eine verpflichtende Anweisung, an den entsprechenden Seminaren teilgenommen haben, der Flurfunk funktionierte und letztlich fast alle Mitarbeiter erreicht wurden. Sehr zum Erfolg beigetragen hat auch die Tatsache, dass die vermittelten Inhalte nicht nur am Arbeitsplatz, sondern genauso auch im privaten Umfeld genutzt werden können.

Es hat sich herausgestellt, dass eine erfolgreiche Sensibilisierung nicht nur die Probleme und Gefahren aufzeigen muss, sondern auch konkrete Hinweise zum praktischen Umgang mit Gefährdungen enthalten sollte.

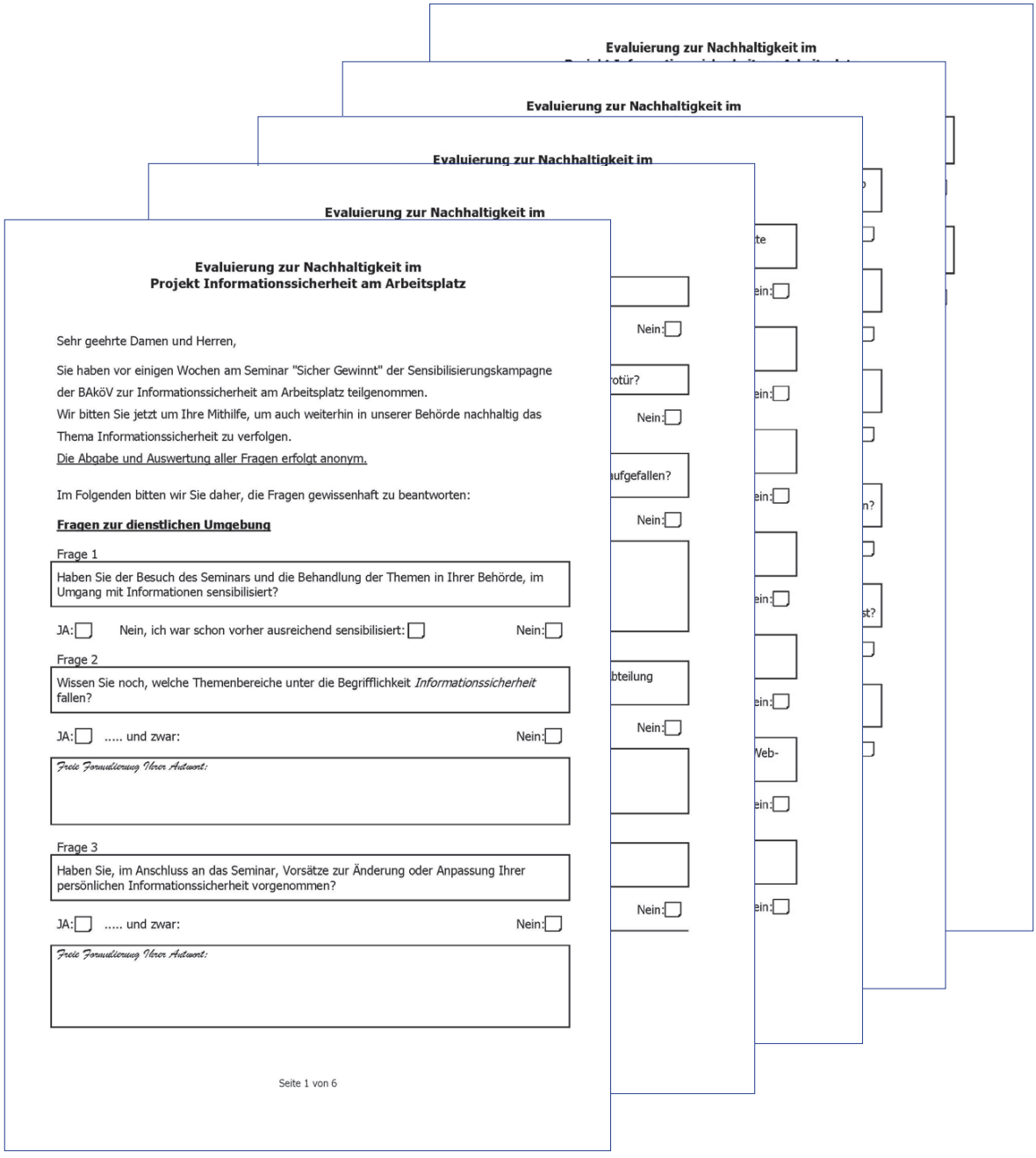
Weiterhin wurden

- die Kenntnisse und die Akzeptanz grundlegender Sicherheitsmaßnahmen, z. B. Umgang mit Passwörtern, gestärkt
- zusätzliche Maßnahmen in den Behörden umgesetzt und von den Mitarbeitern verstanden, wie z. B. VPN-Mail-Zugänge für die THW-Ortsverbände, Sicherung der USB-Schnittstellen, Einführung verschlüsselter USB-Sticks etc.
- die BAköV Lernwelt ins Intranet gestellt
- der BISS auch nach Abschluss der Kampagne weiterhin beworben

Wie geht es weiter: Konzepte zur Nachhaltigkeit

Neben den im vorigen Abschnitt bereits genannten Punkten sind z. B. für die normalen User Wiederholungsschulungen mit unterschiedlichen Schwerpunkten vorgesehen, fast flächendeckend wurde das Thema Informationssicherheit in die Einweisungen für neue Mitarbeiter aufgenommen.

IT-Fachkräfte werden über die Kampagne dazu bewegt, ihr Fachwissen im Bereich der Sicherheit von Betriebssystemen, Netzwerken oder Softwareentwicklung zu vertiefen. In einigen Behörden existierten bereits interne Schulungsunterlagen zum Thema Informationssicherheit. Diese wurden anhand der Feedbacks überarbeitet. Für Führungskräfte sind Folgeseminare zum Thema „Aktuelle Entwicklungen“ und zu rechtlichen Themen geplant.



Evaluierung zur Nachhaltigkeit im
Projekt Informationssicherheit am Arbeitsplatz

Sehr geehrte Damen und Herren,

Sie haben vor einigen Wochen am Seminar "Sicher Gewinnt" der Sensibilisierungskampagne der BAköV zur Informationssicherheit am Arbeitsplatz teilgenommen.
Wir bitten Sie jetzt um Ihre Mithilfe, um auch weiterhin in unserer Behörde nachhaltig das Thema Informationssicherheit zu verfolgen.
Die Abgabe und Auswertung aller Fragen erfolgt anonym.

Im Folgenden bitten wir Sie daher, die Fragen gewissenhaft zu beantworten:

Fragen zur dienstlichen Umgebung

Frage 1
Haben Sie der Besuch des Seminars und die Behandlung der Themen in Ihrer Behörde, im Umgang mit Informationen sensibilisiert?

JA: ☐ Nein, ich war schon vorher ausreichend sensibilisiert: ☐ Nein: ☐

Frage 2
Wissen Sie noch, welche Themenbereiche unter die Begrifflichkeit *Informationssicherheit* fallen?

JA: ☐ ..... und zwar: Nein: ☐

Freie Formulierung Ihrer Antwort:

Frage 3
Haben Sie, im Anschluss an das Seminar, Vorsätze zur Änderung oder Anpassung Ihrer persönlichen Informationssicherheit vorgenommen?

JA: ☐ ..... und zwar: Nein: ☐

Freie Formulierung Ihrer Antwort:

Seite 1 von 6

Schlussbetrachtung

11. Von der Sensibilisierung zur Risikomündigkeit

Dr. Käthe Friedrich, Referentin Bundesakademie für öffentliche Verwaltung (BAköV)

Wer hätte beim Start der Initiative gedacht, dass wir Lernwelten entwickeln, Spiele kaufen oder ein Passworttheater und Live-Hacker in die Behörden schicken würden. Aber wir wurden alle überrascht – vom starken Interesse am Thema und der unerwarteten Resonanz in den Behörden. Offenbar haben wir ein wichtiges Thema zur rechten Zeit aufgegriffen.

Über 40 Berater und Dozenten waren zwei Jahre in fast 100 Behörden tätig. Und es wurde viel erreicht. Wir haben gelernt, Geschichten zu erzählen und die Geschichte als ideales Mittel zur Übermittlung einer rationalen Botschaft zu nutzen. Wir haben diese Geschichten auf verschiedene Weisen erzählt und die Beschäftigten haben das Thema mitgenommen, an den Arbeitsplatz und nach Hause. Ein Prozess, der zur Risikomündigkeit führt, wurde angestoßen.

Wir müssen weiter machen.

Rahmenverträge verlängert

Wir werden die Angebote der BAköV fortsetzen. Die Rahmenverträge mit den externen Dienstleistern wurden verlängert, weitere finanzielle Mittel stehen in einem gewissen Umfang zur Verfügung. Nachdem wir die Sensibilisierung für den Wert der Informationen, mit denen wir täglich umgehen, angestoßen und jedem die eigene Verantwortung und den eigenen Beitrag vermittelt haben, geht es nun darum, risikobewusstes Verhalten stärker in den Fokus zu rücken. Das Ziel muss ein einheitliches Verständnis von sicherheitsbewußtem Handeln sein. Um das zu erreichen, wird die BAköV den Sensibilisierungsprozess in den Behörden weiter unterstützen.

Neue zentrale Angebote im Werkzeugkasten

Das Vertiefen von Themen, das Aufgreifen aktueller Ereignisse und das zielstrebige und methodische Vorgehen in der Sensibilisierung wird die Schwerpunkte prägen. Dazu gehören auch die Unterstützung bei der Bestimmung der Ziele und deren Erreichung und die Evaluation und Auswertung der Ergebnisse zu fördern. Das Angebot von Workshops zum Erfahrungsaustausch und zentralen Veranstaltungen für bestimmte Zielgruppen wird dies ergänzen.

Die Sensibilisierung hat im Prozess der IT-Sicherheit jeder Behörde einen festen Platz gefunden. Die Beschäftigten sind an jedem Arbeitsplatz Bestandteil der Sicherheit der Informationen.

Impressum

Bundesakademie für öffentliche Verwaltung
im Bundesministerium des Innern
– Lehrgruppe 5 –
Willy-Brandt-Str. 1
50321 Brühl

Tel.: 0228/99 629 - 0

E-Mail: sibe-lg5@bakoev.de

Gestaltung
K2G – die Kommunikationsagentur, Berlin
www.k2g.de

Fotos
Titel: Clipdealer
Seiten 6 und 7: aus den Behörden
Seite 10, 18 und 20: privat

Herbst 2011