Die zehn bewährten Praktiken der ENISA im Bereich der Sensibilisierung für Informationssicherheit

Juli 09

enisa
European Network and Information Security Agency

Die ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine Einrichtung der Europäischen Union, die mit dem Ziel errichtet wurde, die Funktionsfähigkeit des Binnenmarktes zu fördern. Als Kompetenzzentrum berät die ENISA die Mitgliedstaaten und die Einrichtungen der Europäischen Union über Netz- und Informationssicherheit, spricht Empfehlungen aus und dient als zentrale Anlaufstelle für Informationen über bewährte Praktiken. Darüber hinaus fördert diese Einrichtung die Kontakte zwischen den Europäischen Institutionen, den Mitgliedstaaten und den Akteuren aus Wirtschaft und Industrie.

Kontakt:

Allgemeine Anfragen zu Sensibilisierungsmaßnahmen zur Informationssicherheit richten Sie bitte an:

E-Mail: Isabella Santa, Leitende Sachverständige für Sensibilisierungsfragen – awareness@enisa.europa.eu

Die zehn bewährten Praktiken der ENISA im Bereich der Sensibilisierung für Informationssicherheit

Juli 2009

Inhalt

Die ENISA 2

ZUSAMMENFASSUNG 5

DIE ZEHN BEWÄHRTEN PRAKTIKEN DER ENISA IM BEREICH DER SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT 6

Verwenden Sie ein Passwort 6
Verwenden Sie ein starkes Passwort 6
Ändern Sie Ihr Passwort regelmäßig 7
Halten Sie Ihr Passwort geheim 7
Verwenden Sie verschiedene Passwörter 7
Schützen Sie Ihren Computer 7
Seien Sie vorsichtig im Umgang mit E-Mail und Internet 7
Seien Sie vorsichtig im Umgang mit tragbaren Geräten Ihrer Organisation: Laptops, USB-Speichersticks, Mobiltelefone und BlackBerrys 8
Laptops 8
USB-Speichersticks 8
Mobiltelefone und BlackBerrys 9
Seien Sie vorsichtig im Umgang mit Daten 9
Besucher 9
Melden Sie Vorfälle sowie Verlust oder Beschädigung tragbarer Geräte Ihrer Organisation 10
Schützen Sie Daten außerhalb Ihrer Organisation 10
Halten Sie sich an die Vorschriften und Verfahren Ihrer Organisation im Zusammenhang mit der Informationssicherheit 10

SCHLUSSFOLGERUNGEN 11

LITERATURVERZEICHNIS 12

Zusammenfassung

Diese Broschüre behandelt wichtige Kernthemen im Bereich der Sensibilisierung für die Sicherheit von Informations- und Kommunikationstechnologien (IKT) in Unternehmen. Hierzu werden bewährte Sicherheitspraktiken erläutert, welche die Aufmerksamkeit der Mitarbeiter auf die Informationssicherheit lenken und sie IT-Sicherheitsprobleme erkennen lassen, auf die sie dann entsprechend reagieren können.

Bewährte Praktiken können als Leitfaden für die zu ergreifenden grundlegenden Maßnahmen bei der Förderung der Sensibilisierung für Informationssicherheit verwendet werden. Die ENISA hat diese Broschüre erstellt, um Mitarbeiter für die Risiken im Bereich der Informationssicherheit zu sensibilisieren und ihnen die zehn goldenen Regeln zu erläutern. Die Broschüre kann für ein Schulungsprogramm zum Thema Informationssicherheit, für eine Sensibilisierungsmaßnahme und auf einer Unternehmens-Website verwendet werden.

Die zehn bewährten Sicherheitspraktiken der ENISA wurden zusammen mit anderen Hilfsmitteln im Rahmen der europaweiten Kampagne der Agentur zur Sensibilisierung für Informationssicherheit entwickelt.

Die zehn bewährten Praktiken der ENISA im Bereich der Sensibilisierung für Informationssicherheit

Verletzungen des Schutzes von Daten, die erst kürzlich großes Medieninteresse erregt haben, gaben Anlass zur Sorge und machten privaten und öffentlichen Organisationen deutlich, dass sensible Unternehmensdaten nur mit Hilfe geeigneter Strategien und Technologien geschützt werden können. Die betreffenden Schutzmaßnahmen müssen einerseits sicherstellen, dass die Daten im Netzwerk geschützt sind, und andererseits die Möglichkeit bieten, die eingehenden und ausgehenden Daten sicher zu verwalten. Geeignete Strategien und Technologien bilden zwar einen wesentlichen Bestandteil eines jeden Programms für Informationssicherheit, reichen allein jedoch nicht aus, um in der Praxis eine ausreichende Informationssicherheit zu gewährleisten.

Das Bewusstsein hinsichtlich der bestehenden Risiken und der verfügbaren Schutzmechanismen bildet die erste Verteidigungslinie zum Schutz der Daten. Die Mitarbeiter sind die eigentliche Schnittstelle zum Netzwerk einer Organisation, daher ist ihr Verhalten ein wesentlicher Aspekt des gesamten Sicherheitsumfelds. Der Schutz von Organisationen setzt bei den Mitarbeitern an. Die Mitarbeiter müssen ihre Aufgaben und Zuständigkeiten im Zusammenhang mit dem Schutz sensibler Daten und der Unternehmensressourcen kennen und in ihrer Organisation einen Beitrag zur Sicherheit von Computern und Netzwerk leisten.

Zu diesem Zweck ist die ENISA bemüht, das Verhalten der Mitarbeiter hinsichtlich Informationssicherheit positiv zu beeinflussen und die Einstellung der Menschen im Sinne eines stärkeren Bewusstseins für die Informationssicherheit zu verändern.

Aus diesem Grund hat die Agentur diese Broschüre mit den zehn bewährten Sicherheitspraktiken erstellt. Diese bewährten Praktiken eignen sich hervorragend, um Mitarbeiter für die Risiken im Bereich der Informationssicherheit zu sensibilisieren und ihnen die zehn goldenen Regeln zu erläutern.

Das vorliegende Dokument richtet sich an Organisationen, die mit der Durchführung von Initiativen beauftragt sind, die den Mitarbeitern zeigen, wie sie die Daten und Vermögenswerte von Unternehmen proaktiv schützen.

1. Verwenden Sie ein Passwort

Mit Ihrem Passwort schützen Sie Ihre Daten vor unberechtigtem Zugriff, so wie Sie Ihr Haus abschließen, um Eindringlinge fernzuhalten. Passwörter stellen einen wichtigen Schutzmechanismus dar, daher helfen Ihnen bewährte Praktiken im Zusammenhang mit dem Passwort, Ihre sensiblen persönlichen Daten und Ihre Identität besser zu schützen.

Verwenden Sie ein starkes Passwort

- ✓ Das Passwort zu Ihrem Desktop gewährt Zugriff auf alle persönlichen und Unternehmensdaten, die Sie auf Ihrem Computer gespeichert haben, und auf alle Online-Konten. Verwenden Sie ein starkes Passwort, um Ihre Daten zu schützen: Verwenden Sie mindestens acht Zeichen und kombinieren Sie Buchstaben (Groß- und Kleinschreibung), Ziffern und Symbole. Je größer die Zeichenvielfalt in Ihrem Passwort, desto schwieriger ist es zu erraten. Verwenden Sie keine personenbezogenen Informationen wie Ihren Namen, den Namen Ihres Kindes oder einen Geburtstag, die jemand bereits kennt oder

leicht in Erfahrung bringen kann. Versuchen Sie außerdem, gemeinsprachliche Wörter zu vermeiden, weil einige Hacker Programme einsetzen, die jedes Wort ausprobieren, das im Wörterbuch steht.

Ändern Sie Ihr Passwort regelmäßig

- ✓ Wenn Sie den Eindruck haben, dass auf Ihr System unrechtmäßig zugegriffen wurde, ändern Sie sofort Ihre Passwörter.

Halten Sie Ihr Passwort geheim

- ✓ Ihr Passwort ist eindeutig und darf niemandem mitgeteilt werden.
- ✓ Versuchen Sie nach Möglichkeit, sich Ihre Passwörter einzuprägen. Überlegen Sie sich eine Strategie, wie Sie sich die Passwörter merken können.
- ✓ Wenn Sie Ihre Passwörter notieren, bewahren Sie sie sicher auf. Legen Sie die Aufzeichnung Ihrer Passwörter nur dort ab, wo Sie auch die Daten ablegen würden, die die Passwörter schützen.

Verwenden Sie verschiedene Passwörter

- ✓ Verwenden Sie für jedes Online-Konto, auf das Sie zugreifen, ein anderes Passwort (oder verwenden Sie zumindest mehrere verschiedene Passwörter). Wenn Sie für mehrere Konten dasselbe Passwort verwenden, hat ein Angreifer, der sich Zugriff auf eines Ihrer Konten verschafft, Zugang zu allen Ihren Konten.

2. Schützen Sie Ihren Computer

- ✓ Schützen Sie Ihren Desktop vor unbefugtem Zugriff, wenn Sie Ihren Platz verlassen, um in eine Besprechung, eine kurze Pause oder die Mittagspause zu gehen.
- ✓ Lassen Sie nicht zu, dass andere Personen ihren USB-Speicherstick an Ihren Computer anstecken, insbesondere wenn es sich um private, nicht gesicherte Speichersticks handelt.
- ✓ Installieren Sie keine illegale oder nicht genehmigte Software, denn damit gefährden Sie die Datensicherheit und verstoßen gegen das Gesetz. Unbekannte Programme von außen können im Netzwerk Ihrer Organisation zu Sicherheitsrisiken führen.
- ✓ Schließen Sie keine privaten Laufwerke, Musikabspielgeräte oder USB-Speichersticks an Ihren Arbeitsplatzrechner an.
- ✓ Schließen Sie Ihren privaten Laptop nicht an das Netzwerk Ihrer Organisation an, da er mit Viren oder Malware infiziert sein könnte.

3. Seien Sie vorsichtig im Umgang mit E-Mail und Internet

- ✓ Öffnen Sie keine E-Mails und Anhänge von unbekannten Absendern.
- ✓ Öffnen Sie in verdächtigen E-Mails keine Hyperlinks.
- ✓ Leiten Sie E-Mails bei Bedarf weiter. Erwägen Sie jedoch, zuvor die Nachrichtenhistorie zu löschen.
- ✓ Nutzen Sie nur Dokumente im PDF-Format gemeinsam, um sicherzustellen, dass die Dateien nicht einfach geändert werden können.

- ✓ Vertrauliche Informationen sollten verschlüsselt werden, bevor sie per E-Mail versendet werden.
- ✓ Seien Sie vorsichtig, wenn Sie im Internet surfen.
- ✓ Geben Sie in Internetforen keine Informationen über Ihre Organisation und Ihre Arbeit preis.
- ✓ Schreiben Sie keine Blogs, bei denen Ihre Ansichten und Meinungen als die Ihrer Organisation ausgelegt werden könnten.
- ✓ Laden Sie keine Dokumente und Materialien herunter, deren Quellen nicht vertrauenswürdig sind.
- ✓ Vermeiden Sie es, Material mit illegalem oder anstößigem Inhalt zu öffnen, herunterzuladen, zu speichern oder zu versenden.
- ✓ Denken Sie daran, dass die Internetseiten, die Sie von Ihrem Arbeitsplatz aus aufrufen, zurückverfolgt werden können.

4. Seien Sie vorsichtig im Umgang mit tragbaren Geräten Ihrer Organisation: Laptops, USB-Speichersticks, Mobiltelefone und BlackBerrys

Laptops

- ✓ Installieren Sie keine illegale oder nicht genehmigte Software, denn damit gefährden Sie die Datensicherheit und verstoßen gegen das Gesetz.
- ✓ Unterbrechen Sie drahtlose Verbindungen, wenn Sie diese nicht benötigen.
- ✓ Schließen Sie Ihren Laptop regelmäßig an das Netzwerk Ihrer Organisation an, um Ihre Sicherheitsprüfungen zu aktualisieren.
- ✓ Legen Sie eine Sicherungskopie der auf Ihrem Laptop abgelegten Daten an.
- ✓ Schützen Sie Ihren Laptop vor unbefugtem Zugriff, wenn Sie Ihren Platz verlassen, um in eine Besprechung, eine kurze Pause oder die Mittagspause zu gehen.
- ✓ Lassen Sie nicht zu, dass andere Personen ihren USB-Speicherstick an Ihren Laptop anstecken, insbesondere wenn es sich um private, nicht gesicherte Speichersticks handelt.
- ✓ Lassen Sie Ihren Laptop nicht unbeaufsichtigt.
- ✓ Lassen Sie Ihren Laptop nicht sichtbar im Auto liegen.

USB-Speichersticks

- ✓ Verwenden Sie einen verschlüsselten USB-Speicherstick.
- ✓ Speichern Sie Unternehmensdaten nur in begrenztem Maße auf Ihrem USB-Speicherstick, vor allem, wenn Sie einen privaten, nicht gesicherten Speicherstick verwenden.
- ✓ Befestigen Sie Ihre USB-Speichersticks an Schlüsselringen oder Tragebändern, um sie nicht zu verlieren; aufgrund ihrer geringen Größe gehen sie sehr leicht verloren oder können leicht gestohlen werden. Außerdem erhöhen größere Speicherkapazitäten die potenziell dem Risiko eines unberechtigten Zugriffs ausgesetzte Datenmenge. USB-Speichersticks werden gewöhnlich in Handtaschen, Rucksäcken, Laptop-Taschen, Jackett- oder Hosentaschen aufbewahrt oder unbeaufsichtigt am Arbeitsplatz zurückgelassen. In jüngerer Zeit ist es wiederholt zu Vorfällen gekommen, da USB-Speichersticks immer wieder verloren, verlegt, ohne Erlaubnis ausgeliehen oder gar gestohlen werden.
- ✓ Legen Sie den Benutzern von USB-Speichersticks nahe, diese im Read-Only-Modus zu betreiben, um das Übertragen von Viren zu vermeiden: An einigen

USB-Sticks befindet sich ein Schalter bzw. eine Verriegelung, um das Gerät in den Read-Only-Modus zu versetzen, der das Beschreiben des Laufwerks bzw. das Ändern darauf gespeicherter Daten durch den Host-Rechner verhindert.

- ✓ Unterziehen Sie den USB-Speicherstick einem Anti-Virus-Scan, wenn Sie Dateien von einem nicht vertrauenswürdigen oder nicht genehmigten Rechner kopiert haben.
- ✓ Bevor Sie Ihren USB-Speicherstick an den PC einer anderen Person anstecken, löschen Sie alle Dateien, die Sie für den betreffenden Vorgang nicht benötigen.
- ✓ Legen Sie Sicherheitskopien an, um auf USB-Speichersticks abgelegte Daten bei Bedarf wiederherstellen zu können.

Mobiltelefone und BlackBerrys

- ✓ Unterbrechen Sie drahtlose Verbindungen (d. h. Bluetooth und WLAN), wenn Sie diese nicht nutzen. Mit Hilfe der Bluetooth-Technologie können elektronische Geräte per Funkvernetzung über kurze Distanz miteinander kommunizieren. Einige Bluetooth-Mobiltelefone sind von Softwarefehlern betroffen, die Bluejacking und Bluesnarfing ermöglichen.
  Bluejacking bedeutet das anonyme Versenden elektronischer Visitenkarten, die eine Nachricht enthalten, an andere Bluetooth-fähige Geräte. Bluejacking wird betrieben, um unangeforderte Nachrichten zu versenden.
  Bluesnarfing wird betrieben, um auf die persönlichen Daten (z. B. Kontaktdaten) in einem Mobiltelefon zuzugreifen und in ein anderes Mobiltelefon zu kopieren.
- ✓ Lassen Sie Ihre Mobiltelefone und BlackBerrys nicht unbeaufsichtigt. Bedenken Sie, dass Sie andernfalls Daten verlieren können.

5. Seien Sie vorsichtig im Umgang mit Daten

- ✓ Kennzeichnen Sie jedes Dokument mit dem jeweiligen Klassifizierungscode.
- ✓ Schützen Sie sensible Daten mit einem Passwort, damit sie nicht von unbefugten Personen geändert oder gelöscht werden können.
- ✓ Halten Sie Ihren Schreibtisch in Ordnung und lassen Sie sensible Daten nicht offen herumliegen. Entsorgen Sie Dokumente sorgfältig.
- ✓ Lassen Sie sensible Daten nicht in gemeinsam genutzten Konferenz- oder Sitzungsräumen liegen, damit sie nicht für Personen zugänglich sind, die den Raum nach Ihnen nutzen.
- ✓ Sicheres Drucken: Drucken, kopieren und scannen Sie Daten nur, wenn dies wirklich nötig ist. Lassen Sie das Dokument nicht im Drucker liegen.
- ✓ Vernichten Sie stets Dokumente, die sensible Daten enthalten oder als vertraulich gekennzeichnet sind.
- ✓ Legen Sie keine Daten auf Ihrer lokalen Festplatte ab.
- ✓ Stellen Sie sicher, dass jeder Dritte, der mit Ihnen zusammenarbeitet, eine Geheimhaltungsvereinbarung unterzeichnet hat, bevor Sie ihm sensible Daten zugänglich machen.

6. Besucher

- ✓ Alle Besucher sollten bei ihrer Ankunft registriert und angemeldet und bei Verlassen des Gebäudes wieder abgemeldet werden.
- ✓ Alle Besucher sollten einen Besucherausweis erhalten, den sie während ihres

Besuchs im Unternehmensgebäude zu jeder Zeit tragen müssen.

- ✓ Begleiten Sie Besucher zu jeder Zeit während ihres Aufenthaltes im Unternehmensgebäude. Besucher in den Büroräumen unbeaufsichtigt zu lassen, kann zu Risiken führen.

7. Melden Sie Vorfälle sowie Verlust oder Beschädigung tragbarer Geräte Ihrer Organisation

- ✓ Benachrichtigen Sie die IT-Abteilung Ihrer Organisation über Verlust oder Beschädigung tragbarer Geräte Ihrer Organisation (Mobiltelefone, PDAs oder USB-Speichersticks).
- ✓ Benachrichtigen Sie die IT-Abteilung Ihrer Organisation, wenn Sie ein tragbares Gerät Ihrer Organisation gefunden haben.
- ✓ Melden Sie alle Verstöße und Vorfälle im Zusammenhang mit der Informationssicherheit, auch wenn Sie nicht ganz sicher sind.
- ✓ Melden Sie es, wenn Ihnen an Ihrem Arbeitsplatz etwas verdächtig vorkommt oder wenn eine Anwendung plötzlich nicht mehr verfügbar ist, ohne dass Ihre IT-Abteilung Sie vorab darüber informiert hat.

8. Schützen Sie Daten außerhalb Ihrer Organisation

- ✓ Stellen Sie sicher, dass Sie sensible Daten und Geräte jederzeit sicher aufbewahren, wenn Sie sich außerhalb Ihrer Organisation befinden, um Diebstahl oder Verlust zu vermeiden. Seien Sie vor allem in der Öffentlichkeit vorsichtig im Umgang mit Daten.
- ✓ Beachten Sie, dass andere Personen mithören können, was Sie sagen. Machen Sie sensible Informationen Ihrer Organisation nicht für jeden zugänglich.
- ✓ Wenn Sie unterwegs oder von einem dezentralen Arbeitsplatz aus arbeiten, achten Sie darauf, dass Ihnen niemand über die Schulter schauen kann. Schützen Sie sich vor Shoulder-Surfing.

9. Halten Sie sich an die Vorschriften und Verfahren Ihrer Organisation im Zusammenhang mit der Informationssicherheit

- ✓ Halten Sie sich an die geltenden Vorschriften und Verfahren Ihrer Organisation im Zusammenhang mit der Informationssicherheit.
- ✓ Stellen Sie die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicher.
- ✓ Beachten Sie die rechtlichen Anforderungen, wie urheberrechtliche Beschränkungen, Rechte an geistigem Eigentum, Recht auf Privatsphäre und Softwarelizenzen.
- ✓ Melden Sie unverzüglich, wenn Sie sehen, dass Kollegen gegen die Vorschriften und Verfahren Ihrer Organisation im Zusammenhang mit der Informationssicherheit verstoßen.

10. Tragen Sie durch Rückmeldung zu einer Verbesserung der vorgeschriebenen Lösungen und Sicherheitsvorschriften bei

- ✓ Tragen Sie durch Rückmeldung zu einer Verbesserung der vorgeschriebenen Lösungen und Sicherheitsvorschriften bei.
- ✓ Regen Sie die Anschaffung zusätzlicher Software an, wenn Sie diese für Ihre Arbeit benötigen.
- ✓ Stellen Sie Fragen oder machen Sie Vorschläge, die der Verbesserung von Lösungen und Sicherheitsvorschriften dienen.

Schlussfolgerungen

Informationen müssen vor unerlaubtem Zugriff geschützt werden, und die Mitarbeiter müssen ihre Aufgaben und Zuständigkeiten im Zusammenhang mit dem Schutz sensibler Daten und der Vermögenswerte des Unternehmens kennen.

Die Mitarbeiter müssen sich bewusst sein, was sie mit nach Hause nehmen dürfen und was nicht (unternehmenseigene Laptops usw.), welche Befugnisse sie im Zusammenhang mit Unternehmensressourcen haben und inwieweit sie Sicherungskopien erstellen und Sicherheitstechnologie nutzen müssen.

Zu diesem Zweck ist die ENISA bemüht, das Verhalten der Mitarbeiter hinsichtlich Informationssicherheit positiv zu beeinflussen und die Einstellung der Menschen im Sinne eines stärkeren Bewusstseins für die Informationssicherheit zu verändern.

Die Beachtung der bewährten Praktiken im Bereich Sensibilisierung für Informationssicherheit lenkt die Aufmerksamkeit der Mitarbeiter auf die Informationssicherheit und lässt sie die häufigsten Sicherheitsrisiken der Informationstechnologie erkennen und entsprechend darauf reagieren.

Literaturverzeichnis

ENISA, *Sicherer Umgang mit USB-Speichersticks*, Juni 2008, abrufbar unter http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-usb-flash-drives-de

ENISA, *Sicheres Drucken*, April 2008, abrufbar unter http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing-de

Die zehn bewährten Praktiken der ENISA im Bereich der Sensibilisierung für Informationssicherheit

ISBN-13: 978-92-9204-045-1

DOI: 10.2824/18503

Katalognummer: TP-80-10-258-DE-N

TP-80-10-258-DE-N

ISBN-13 978-92-9204-045-1

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu