Mit SecureAware®
Informationssicherheit verwalten

Beschreibung der Konzeption

Inhalt

Einleitung 3
Informationssicherheit 4
Der Vergleich 4
  Drei Voraussetzungen für Sicherheit 5
  Mittel und Methoden die Informationssicherung zu erhöhen 5
Wie man SecureAware im Management der Informationssicherheit einsetzt 6
  Mit Policies arbeiten 7
  Awarenessprogramme 9
  Informationsaustausch zwischen den drei Modulen von SecureAware 10
  Themenbereiche - Inhaltskategorien 11
  Zielgruppen 11
Eigenschaften und Vorteile von SecureAware 12
Weitergehende Informationen 13

Einleitung

Dieses Papier beschreibt die Bedrohungen der Informationssicherheit, denen viele Organisationen ausgesetzt sind und führt in die Konzeption ein, die hinter SecureAware steht.

SecureAware ist ein System zur Verwaltung von Informationssicherheit. Die Computeranwender erhalten die notwendigen Informationen, lernen die Grundlagen der Informationssicherheit und erwerben das notwendige Sicherheitsbewusstsein. SecureAware spart Zeit und damit Geld, wenn Sicherheitsbeauftragte und Organisationen mit IT-Security Policies und Awarenessprogrammen arbeiten. Die Unternehmensziele sind sichtbar verbunden mit Sicherheitsregeln und Verfahrensvorschriften. Zugleich sind diese Regeln mit der Ausbildung der Mitarbeiter verbunden. Das ganze System hilft Organisationen eine menschliche Firewall zu bauen - die Mitarbeiter gewährleisten die Informationssicherheit aktiv mit anstatt das schwächste Glied in der Kette der Sicherheitsmaßnahmen darzustellen.

Informationssicherheit

Einhundertprozentige Sicherheit gibt es nicht. Aber es ist durchaus möglich die Anzahl unerwünschter Sicherheitsvorfälle zu reduzieren, und damit auch deren Folgen einschließlich der wirtschaftlichen Folgen.

Unternehmensmanagement ist zugleich Risikomanagement. Zuviel oder zuwenig Aufwand für Sicherheit kann ein Unternehmen zerstören. Wenn Firmen ihre Risiken abschätzen und Gegenmaßnahmen erwägen, so kommen sie immer zum Ergebnis, dass **technische Lösungen allein keinen ausreichenden Schutz bieten** können. Virusschutz-Produkte, Firewalls und Betriebssysteme können nicht so schützen, wie es die meisten Organisationen benötigen.

In der Kette von Sicherheitsmaßnahmen bilden Produkte wie Firewalls, Virusschutz-Software, Verschlüsselungslösungen, Netzwerkprodukte, Betriebssysteme und Software wie Internetbrowser oder e-Mailclients die technologischen Glieder. Die menschlichen Glieder sind die Computeruser: Menschen die mit Informationen arbeiten und Computer bei ihrer Arbeit anwenden. Beide Teile der Kette sind gleich wichtig für die Informationssicherheit.

Menschliches Verhalten oder Fehlverhalten beeinflusst die Informationssicherheit eines Unternehmens genauso wie die technologischen Lösungen, die zur Sicherung der Informationen angeschafft wurden.

Und solange Menschen an Computern arbeiten, kann es keine rein technologische Lösung des Sicherheitsproblems geben.

Jeder weiß, dass jede Kette so schwach ist wie das schwächste Glied. Trotzdem werden die menschlichen Kettenglieder allzu oft übersehen. Es scheint doch offensichtlich und von größter Wichtigkeit zu sein, dass man das Sicherheitswissen und Sicherheitsbewusstsein der Mitarbeiter im Bereich der Informationssicherheit erhöhen muss. Trotzdem gibt es kaum verwendbare Lösungen auf dem Markt, d.h. Lösungen, die das "schwächste Glied" in der Kette der Sicherheit wirksam stärken.

Den Mitarbeitern zu helfen, die wertvollen Informationen ihres Unternehmens effektiv zu schützen erfordert wohldefinierte und auch tatsächlich bekannt gemachte Policies und Verfahrensmaßnahmen sowie Awarenessprogramme.

Der Vergleich

Stellen Sie sich den Straßenverkehr ohne Verkehrsregeln vor. Verkehrsregeln sorgen für Verkehrssicherheit. IT-Sicherheitsregeln sorgen für IT-Sicherheit. So einfach ist das!

Natürlich haben Sie recht mit der Meinung, dass der Verkehr nie ganz sicher ist. Doch weil die meisten Menschen im großen und ganzen die Verkehrsregeln einhalten, verbessern Regeln die Sicherheit. Es wäre bestimmt viel schlechter, wenn die Hälfte von uns auf der verkehrten Straßenseite fahren oder bei Rot einfach weiterfahren würde.

Genauso ist es auch mit Computern und IT-Sicherheit; wir müssen beim Computergebrauch bestimmte „Verkehrsregeln“ befolgen, um die Informationssysteme auf sichere Weise zu nutzen. Solche Verkehrsregeln gehören in eine Security Policy.

Drei Voraussetzungen für Sicherheit

Voraussetzung	Im Straßenverkehr	Bei der Arbeit mit Computern
Regeln sind vorhanden	Straßenverkehrsvorschriften	Security Policy des Unternehmens
Kenntnis der Regeln	Kenntnis der Verkehrsregeln	Kenntnis der Security Policy
Motivation zur Regelbefolgung	Motivation zur Befolgung wird erhöht durch Information über Gefahren und Risiken des Straßenverkehrs	Motivation zur Befolgung wird erhöht durch Information über Gefahren und Risiken der Computernutzung

Mittel und Methoden die Informationssicherung zu erhöhen

Ziel	Mittel
Security Policy definieren und aufrecht erhalten	Offizielle Standards umschreiben Best Practices. Verwenden Sie ein Tool mit Vorlagen, das Ihnen dabei hilft genau diejenigen Policies auszuwählen, die für Ihr Unternehmen richtig sind. Risikoanalyse und Policyinhalte sind zu verknüpfen.
Kenntnis der Policies vermitteln	Erstellen Sie Awarenessprogramme für alle betroffenen Mitarbeiter. Denken Sie daran, dass Sicherheit ein Prozess ist, nicht einfach ein Ergebnis. Setzen Sie die Programme so auf, dass Informationssicherheit immer wieder einmal präsentiert wird. Beanspruchen Sie nicht zuviel Zeit Ihrer Kollegen. Überfordern Sie sie auch nicht - bitten Sie die Mitarbeiter also nicht gleich alle Regeln über Informationssicherheit zu lesen. Viel besser ist, eine Themenliste aufzustellen und immer je nur ein Thema durchzunehmen. Erklären Sie in einem Monat e-Mail zu Thema des Monats, im nächsten Passwörter usw. Registrieren Sie die Ergebnisse der Tests und wiederholen Sie die Themen nach Bedarf (halbjährlich oder jährlich).
Motivieren Sie zur Befolgung	Bringen Sie den Mitarbeitern Informationssicherheit bei. Erzeugen Sie eine Unternehmenskultur zu der Sicherheitswissen und Sicherheitsbewusstsein gehört. Übertreiben Sie nicht – versuchen Sie also nicht alle Kollegen zu Experten in Informationssicherheit zu machen. Jeder soll gerade soviel wissen, wie nötig ist um mit den Daten und Informationen des Unternehmens in sicherer Weise umzugehen. E-Learning macht Lernen kosteneffektiv, auch in großen Unternehmen und Behörden. Weil die Lektionen animiert und vertont sind, wird die Aufmerksamkeit der Mitarbeiter gefangen und sie lernen schneller. Problemlos kann so der gesamten Belegschaft die gleiche Informationen vermittelt werden. Setzen Sie außerdem Themen der Informationssicherheit auf die Tagesordnung von Mitarbeiterbesprechungen um das e-Learning zu ergänzen.

Wie man SecureAware im Management der Informationssicherheit einsetzt

SecureAware besteht aus drei Modulen. Diese drei Module von SecureAware sind miteinander verknüpft. **SecureAware Policy** verwaltet Policies zur Informationssicherheit; **SecureAware Survey** erstellt Awarenessprogramme auf der Grundlage der Policies; **SecureAware Education** vermittelt den Mitarbeitern das notwendige Wissen über Informationssicherheit.

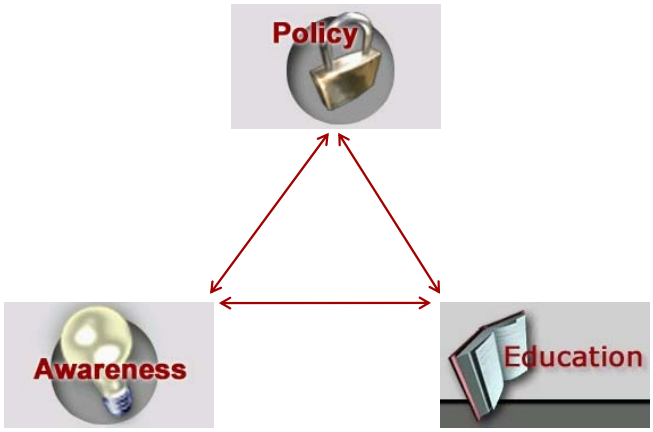

Abbildung: Modulare Struktur

Mit Policies arbeiten

Mit dem Policymodul erstellt, verwaltet und veröffentlicht man Policies zur Informationssicherheit. Der Inhalt ist nach den international anerkannten Standards ISO 17799 und BS 7799 aufgebaut. Vorlagen werden mitgeliefert. Alle Arbeiten an den Regeln werden in einer Log-Datei aufgezeichnet und sind deshalb jederzeit rekonstruierbar. Die Regeln werden dann im Intranet veröffentlicht. Der Zugriff erfolgt einfach über Browser, die bereits auf jedem Computer installiert sind.

Die Sicherheitsbeauftragten erstellen die Policies in **drei Ebenen**:

Die **erste** Ebene definiert eine allgemeine **Strategie** des Unternehmens bzw. der Behörde, in der dargelegt wird, **warum** und inwiefern Informationssicherheit für die jeweilige Organisation wichtig ist.

Die **zweite** Ebene legt in **Sicherheitsregeln** fest, **was** genau vorgeschrieben, erlaubt oder verboten ist.

Die **dritte** Ebene beschreibt in **Verfahrensregeln**, **wie** genau die Organisation und ihre Mitarbeiter die auf der Strategie basierenden Regeln umsetzen.

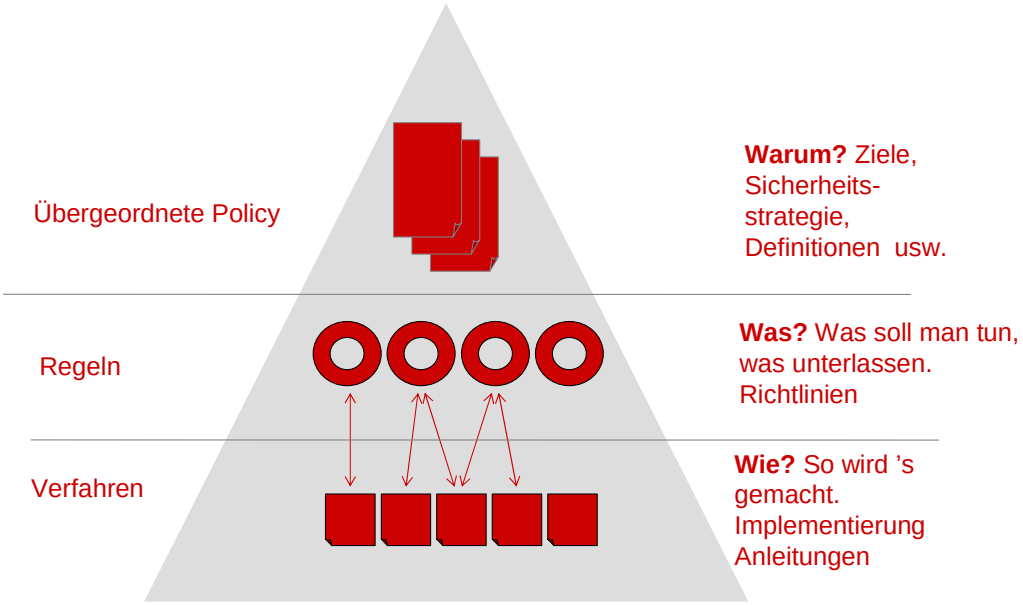

Abbildung: Drei Ebenen des Sicherheitsmanagements

Auf der **obersten Ebene** wird also die generelle **Unternehmens- bzw. Behördenstrategie** zur Informationssicherheit festgelegt. Man wird hier die Ziele des Informations-Sicherheits-Managements-Systems des Unternehmens bzw. der Behörde umschreiben, den Anwendungsbereich festlegen und mitteilen, warum Informationssicherheit für die Organisation so wichtig ist. Der Umfang dieses Strategietextes sollte relativ kurz sein (ca. 2 Textseiten).

Die **mittlere Ebene** - also die Ebene der **Sicherheitsregeln** - besteht aus einzelnen Objekten. Das Besondere an SecureAware ist, dass es sich dabei nicht einfach um Texte handelt, sondern eine **objektorientierte Datenbank**.

Diese Objekte umschreiben, was bei der Anwendung der Informationssysteme erlaubt ist, was nicht erlaubt ist und welche Maßnahmen vorgeschrieben sind. Die Objekte können in verschiedenster Weise strukturiert und bearbeitet werden. Man kann z.B. innerhalb einer einheitlichen Policy für die gesamte Organisation unterschiedliche Regeln für verschiedene Mitarbeitergruppen festlegen. Mit SecureAware werden bereits Standardobjekte zu allen in ISO 17799/BS 7799 vorgesehenen Bereichen mitgeliefert - eine diesem Standard entsprechende Policy kann deshalb mit wenigen Klicks erstellt werden. Der Anwender kann diese Objekte beliebig anpassen, neue hinzufügen oder vorhandene "ausschalten" - auch neue Themenbereiche können eingefügt werden.

Die **untere Ebene** ist die der **Verfahrensregeln**. Diese beschreiben, wie die Sicherheitsrichtlinien umzusetzen sind. Sie geben konkrete Anleitungen zu einzelnen Punkten oder legen fest, durch welche Maßnahmen und in welcher Reihenfolge die Sicherheitsregeln durchgeführt werden sollen. Eine Sicherheitsregel (ein Objekt) kann mit einer oder mehreren Verfahrensmßnahmen verknüpft werden. Und umgekehrt kann durch eine Verfahrensmaßnahme eine oder auch mehrere Sicherheitsregeln umgesetzt werden - und deshalb mit mehreren verknüpft werden. Bei SecureAware werden diese Verfahrensregeln in einer Bibliothek gepflegt. Die Beschreibungen der Verfahren können entweder direkt in der SecureAware-Datenbank gespeichert werden oder es verweist ein Link auf die entsprechende Stelle im Intranet oder Internet. Vorhandene Dokumente oder Materialien werden so in SecureAware integriert.

SecureAware wird so zu einem **umfassenden elektronischen Sicherheitshandbuch**, das in seiner Komplexität genau den jeweiligen Bedürfnissen des Unternehmens bzw. der Behörde entspricht.

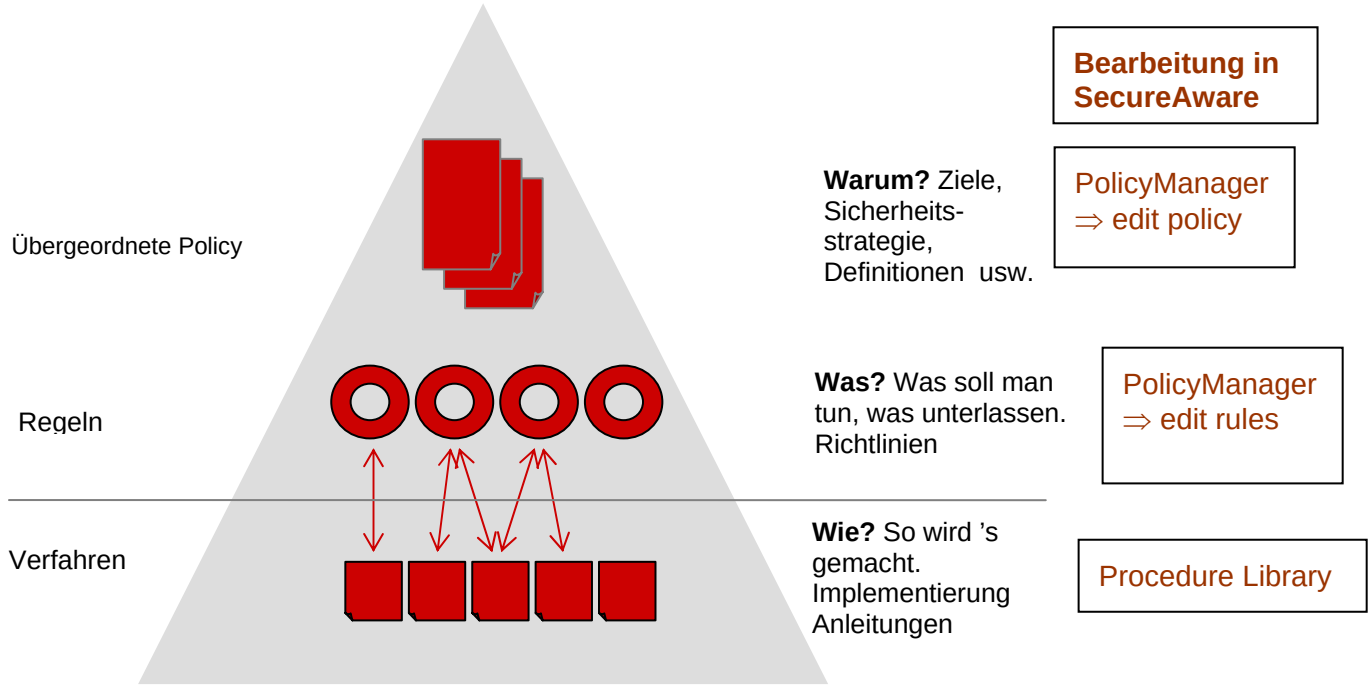

Abbildung: Wie man die drei Ebenen im Policymodul von SecureAware nutzt

Awarenessprogramme

SecureAware ist nicht nur ein innovatives Instrument zur Erstellung und Verwaltung von Security Policies. Das wirklich Einzigartige an SecureAware ist die Verbindung eines Werkzeuges für Sicherheitsrichtlinien mit einem für Awarenessprogramme.

Beim Design von SecureAware sind wir davon ausgegangen, dass es nicht genügt, Sicherheitsstrategie, Sicherheitsrichtlinien und Verfahrensmaßnahmen festzulegen. Die Mitarbeiter müssen die für sie geltenden Regeln auch tatsächlich anwenden. Dazu müssen sie diese Regeln kennen, verstehen und akzeptieren.

Mitarbeiter, die Regeln nicht kennen oder nicht verstehen, verhalten sich entweder unbewusst falsch, oder sie sehen die Regeln als „unnötiger Aufwand“, „Gängelei“ oder „Beschneidung persönlicher Freiheit“ an. Effektivität am Arbeitsplatz und persönliche Interessen kollidieren scheinbar mit Sicherheitsmaßnahmen.

Bloße Befehle oder Zwang verleiten zu Umgehung von Sicherheitsmaßregeln. Erforderlich ist Verstehen und Akzeptanz.

Notwendig ist also zunächst einmal eine Schulung in den Grundlagen und Grundproblemen der Informationssicherheit. Hierzu dienen die Lerninhalte von SecureAware Education. Hier wird der Hintergrund von Maßnahmen zur Informationssicherheit verständlich gemacht. Ob diese Inhalte wirklich verstanden wurden, wird durch Tests in SecureAware Education ermittelt.

SecureAware erstellt diese Tests automatisch nach dem Zufallsprinzip aus einem mitgelieferten Inhalt und sorgt für die Erfassung der Testergebnisse mit allen notwendigen Daten. Eine Anpassung der Grundkonstellation dieser Tests (Thema, Anzahl der Fragen und Schwierigkeitsgrad des Tests) ist eine Sache von wenigen Minuten.Darüber hinaus ist der Inhalt dieser Tests beliebig editierbar.

Aufbauend auf dem so gewonnenen Grundwissen wird die Kenntnis der jeweils aktuellen Sicherheitsregeln des entsprechenden Themenbereiches getestet. Auch dieses policyspezifischen Tests werden vom Programm automatisch erstellt und sind konfigurierbar.

Nur mit SecureAware ist diese Verbindung von generellem Wissen und unternehmensspezifischen Regeln so einfach möglich.

Wir empfehlen in regelmäßigen Zeitabständen - z.B. monatlich - je ein Awarenessprogramm zu einem bestimmten Thema einzusetzen. So wird Informationssicherheit zu einem ständig präsenten Thema im Unternehmen ohne Mitarbeiter vom Zeit- und Verständnisaufwand her zu überfordern. Dies sichert effektive Resultate.

Ziel ist nicht, Experten für Informationssicherheit auszubilden, Mitarbeitern einem Prüfungsdruck auszusetzen oder ihnen Restriktionen aufzuzwingen. Ziel ist, Verständnis für die notwendigen Sicherheitsmaßnahmen zu schaffen und Beschäftigte zur Mithilfe zu motivieren. Nur wohlinformierte und entsprechend motivierte Mitarbeiter können in ihren eigenen Arbeitsbereichen verantwortlich für Informationssicherheit sorgen.

Im folgenden wird die entsprechende Funktionsweise von SecureAware näher erläutert.

Informationsaustausch zwischen den drei Modulen von SecureAware

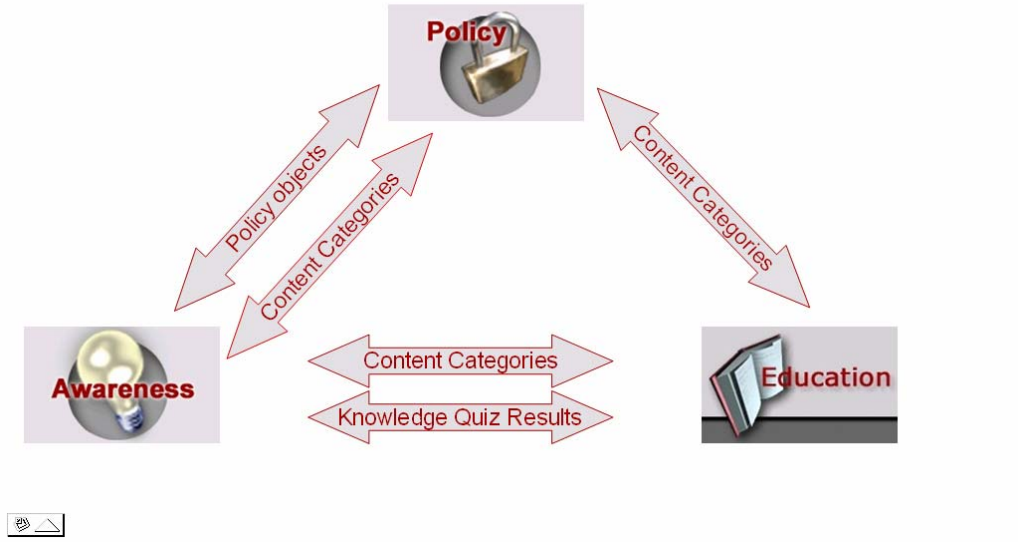

Abbildung: Informationsaustausch zwischen den Modulen

Sicherheitsregeln der Policy, Lehrinhalte und Tests der drei SecureAware-Module werden mittels der Awarenessprogramme miteinander verbunden. Diese Struktur ermöglicht Awarenessprogramme, die die jeweilige Security Policy einbeziehen.

Die Datenbankobjekte, aus denen die aktuelle Policy besteht, werden auch im Modul SecureAware Survey eingesetzt. Die entsprechenden Regeln der Policy werden in den Awareness-Tests verwendet. SecureAware Survey kennt die richtigen Antworten zu den Testfragen, indem es die Regeln der Policy liest. Deshalb braucht der Verantwortliche die Testfragen und Antworten nicht selbst zu schreiben - SecureAware erledigt dies automatisch. Darüber hinaus wird automatisch für eine Übereinstimmung der aktuellen Policy mit den Tests gesorgt: Jede Änderung der Policy wirkt sich auf die Tests aus.

Der Lerninhalt von SecureAware ist benutzerfreundlich in 10 verschiedene Themenbereiche aufgeteilt (e-Mail-Gebrauch, Internetnutzung, Mobile Geräte usf.).

In SecureAware Education stehen für jeden dieser Themenbereiche Lektionen zur Verfügung. Jede Lektion umfasst einen animierten und vertonten Flashfilm sowie je eine Reihe übersichtlicher Infotexte.

Gleichzeitig wird jede Sicherheitsregel der Policy einem oder mehreren dieser Themenbereiche zugeordnet. In Verbindung mit den Lektionen kann der Mitarbeiter deshalb genau die einschlägigen Regeln der Policy heranziehen.

Die Themenbereiche werden auch bei den Awareness-Tests verwendet, die SecureAware Survey automatisch erzeugt. Die Fragen und Antworten der Tests kommen aus zwei verschiedenen Quellen.

Eine Quelle ist ein Pool von generellen (also nicht unternehmensspezifischen) Fragen und Antworten zur Informationssicherheit. Diese Fragen und Antworten werden bereits mit SecureAware mitgeliefert, deshalb werden die Tests ohne zusätzlichen Arbeitsaufwand automatisch erstellt (alle Fragen und Antworten sind jedoch beliebig editierbar).

Die andere Quelle ist die Datenbank der Sicherheitsregeln von SeucreAware Policy selbst. Aus ihr bildet das Survey-Modul automatisch policybezogene Tests für den jeweiligen Themenbereich. Sie entsprechen vom Inhalt her deshalb auch immer den jeweils gültigen Sicherheitsregeln. Verwirrende Inkonsistenzen sind daher ausgeschlossen und eine zusätzliche Pflege der Awareness-Programme ist nicht nötig.

Themenbereiche - Inhaltskategorien

Die Themenbereiche (in SecureAware auch als Inhaltskategorien bezeichnet) werden nicht nur dazu verwendet die drei Module zu verbinden. Sie dienen auch dazu Sicherheitsregeln und Verfahrensmaßnahmen übersichtlich zu strukturieren. Die Security Policy von SecureAware hält sich an die umfangreiche Struktur der Standards ISO 17799/BS 7799. Die Themenbereiche geben eine ergänzende Struktur, die für den "einfachen Endanwender" sicherlich leichter zugänglich ist. Der Anwender kann beispielsweise einfach auf das Thema "Passwörter" klicken und so genau die Regeln zu diesem Thema aufrufen - die entsprechenden Verfahrensmaßnahmen sind dann leicht über Links zugänglich. Die Sicherheitsregeln sind dadurch sehr übersichtlich, was wiederum zum Verständnis beiträgt.

Die verantwortlichen Sicherheitsbeauftragten können so einerseits nach den internationalen Standards arbeiten und eine entsprechend komplexe Gesamt-Security Policy aufbauen. Gleichzeitig erstellen sie damit themenspezifische Policies. Im Unterschied zu einem vielfach üblichen Vorgehen, bei dem für jedes Thema einzelne Policies erstellt werden, werden bei SecureAware automatisch Inkonsistenzen ausgeschlossen und Doppelarbeit vermieden. Die Enduser sehen dann nur das, was für sie wirklich wichtig ist.

Zielgruppen

Während die Gesamtstrategie zur Informationssicherheit für alle Mitarbeiter des Unternehmens/der Behörde gilt, betreffen Sicherheitsregeln und Verfahrensmaßregeln bestimmte Zielgruppen.

Wenn eine bestimmte Sicherheitsregel nur für die EDV-Administration relevant ist, wäre es nicht notwendig und ggf. auch eine Überforderung, z.B. von Mitarbeitern der Buchhaltung ihre Kenntnis zu verlangen. Die Aufmerksamkeit der Mitarbeiter soll nur auf die jeweils in ihrem eigenen Arbeitsbereich wichtigen Regeln gerichtet sein.

Der für SecureAware Verantwortliche (Super-User) weist Sicherheitsregeln und Verfahrensmaßnahmen bestimmten Zielgruppen zu. Er kann diese Zielgruppen nach Bedarf konfigurieren (bereits vorgegeben sind Endanwender, IT-Administratoren und Management). Dadurch ist es dann leicht, die entsprechenden Regeln auszufiltern (also z.B. die Passwortregeln für End-Anwender).

In Verbindung mit den Themenbereichen wird so eine reale Übersichtlichkeit und Verständlichkeit der Sicherheitsregeln auch für die "einfachen" Mitarbeiter erreicht.

Sowohl die Gesamtpolicy als auch solche themen- und zielgruppenspezifischen Policies können auch im .pdf- oder .rtf-Format als Datei oder auf Papier ausgegeben werden.

Eigenschaften und Vorteile von SecureAware

Eigenschaft	Vorteil	Ergebnis
Eingebaute Vorlage	Es ist **einfach** eine Security Policy von Grund auf zu erstellen. Die Vorlagen geben einen guten Ausgangspunkt und können dem eigenen Bedarf flexibel angepasst werden.	**Geringe Kosten** bei Erstellung einer zweckmäßigen maßgeschneiderten Security Policy. **Schnelle Erstellung und Aktualisierung** von Security Policy und Regeln.
Hierarchische Security Policy	Deutliche Struktur mit drei Ebenen: 1. Übergeordnete Ziele und Strategie (**warum** haben wir eine Security Policy), die bestimmen 2. spezifische Regeln (**was** ist vorgeschrieben oder erlaubt, was nicht), die verknüpft sind mit 3. konkreten Verfahrensmaßnahmen (**wie** machen wir es).	**Besserer Überblick über Informationssicherheit - bessere Implementation.** Politik und Regeln hängen mit den Verfahrensmaßnahmen zusammen. Das komplette Sicherheitssystem wird **durchschaubar** gemacht.
Objekt-basierte Security Policy	Es ist **einfach** einzelne Objekte der **Entwicklung** des Unternehmens und der Sicherheitslage **anzupassen**.	Eine **stets aktuelle** Security Policy, die Grundlage ist für das **ausgewogen richtige Niveau** der Informationssicherheit.
Inhalt der Objekte wird mitgeliefert	Es ist leicht aus den vorhandenen Bausteinen die jeweils passenden Objekte auszuwählen und evtl. dem eigenen Bedarf anzupassen. Die **Vollständigkeit** der Security Policy ist **immer gewährleistet**.	**Geringerer Arbeitsaufwand** für Erstellung, **weniger Kosten** für Pflege und Aktualisierung.
Stuktur und Inhalt entspricht anerkannten Standards.	Ihre mit SecureAware erstellte Security Policy entspricht **international anerkannten Standards** (BS 7799, ISO 17799). Es ist einfach, evtl. vorhandene Politik und Regeln einzubauen.	**Bekannte Struktur und anerkannter Inhalt** bedeuten, dass andere - z.B. Wirtschaftsprüfer, Kunden, Partner - leichter Ihre Informationssicherheit nachprüfen können.
Redigierbarer Inhalt	Sie können den Inhalt und die Strukturen **beliebig bearbeiten**. Neue Objekte, Kategorien und Unterkategorien können einfach hinzugefügt werden.	**Vollständige Anpassung** an Ihren Bedarf.

Mehrsprachigkeit des Inhalts und des Endanwender-Interfaces.	International operierende Unternehmen können so leicht **alle Mitarbeiter** informieren. Wenn Standardobjekte in einer Sprache ausgewählt werden, werden **automatisch** die entsprechenden Objekte in den anderen Sprachen mitgewählt.	**Einsparung von Übersetzungen, geringere Kosten für Pflege, bessere Kommunikation für Endanwender.** Besser informierte Mitarbeiter, die besser für Sicherheit sorgen.
Zielgruppen-orientierung	Der Inhalt wird auf die verschiedenen Gruppen von Mitarbeitern zugeschnitten, für "einfache" Endanwender, die IT-Abteilung, Telearbeiter usw. Die Anwender brauchen nicht Regeln zu lesen und Verfahren zu lernen, die nicht mit ihren Arbeitsaufgaben zusammenhängen.	**Einsparungen von Personalkosten**, gleichzeitig **bessere Kenntnis** der relevanten Regeln und Verfahren. Weniger Rückfragen.
PDF-Format unterstützt	Die Security Policy kann in **drucker- und mailfreundlichem Format** ausgegeben werden (auch zielgruppenorientiert).	So ist es leicht die Security Policy zu **externen Partnern** zu kommunizieren.
Integration mit SecureAware Survey	Die Objekte aus der Security Policy werden direkt in Awareness-Tests und Analysen verwendet.	Bessere Kenntnis der Regeln. **Kein Aufwand** für die Erstellung von Tests. Das Sicherheitswissen kann **gemessen** werden.
Integration mit SecureAware Education	Die Themen in Ihrer Security Policy stimmen mit den Ausbildungslektionen in SecureAware Education überein.	**Größere Akzeptanz** der Security Policy und bessere Motivation den Regeln zu folgen.
Installation auf einem Server	Es ist nur **eine einzige Installation notwendig** bei beliebig vielen Anwendern.	**Geringster Aufwand** für Softwareinstallation und -pflege

Weitergehende Informationen

Weitergehende Informationen findet man auf unserer Website www.neupart.com.