

Konvergenz von Awareness und Sicherheitstechnik

Security Awareness in Echtzeit

Der geschulte Anwender kann den Schutzbedarf von unternehmens-eigener Information am besten einschätzen. Technisch umgesetzte Schutzmaßnahmen bleiben dennoch unverzichtbar. Für den sicheren Betrieb bedarf es deshalb zweier Säulen: IT-Security-Awareness und technischen Schutzes. Beides lässt sich gut miteinander kombinieren.

Bisher werden Security Awareness und Sicherheitstechnik häufig als zwei unterschiedliche Disziplinen betrachtet, deren Vorgehensweisen und Projekte kaum Berührungspunkte haben. Plakative Äußerungen wie „Die beste Firewall ist unser Mitarbeiter“ lösen in den Unternehmen aber die technische Firewall keineswegs ab. Andererseits sind die besten technischen Sicherheitsmaßnahmen ihr Geld nicht wert, wenn der berechtigte Nutzer aus pragmatischen Gründen (bewusst oder unbewusst) das Schutzziel ignoriert und damit zur größten Schwachstelle wird.

Zeitgerechter Sicherheitshinweis

Mit einem anderen Denkansatz – „User Awareness in Echtzeit“ – lässt sich das Beste aus beiden Welten miteinander kombinieren. Man schlägt damit die Brücke zwischen dem mit Schulungen gefestigten Sicherheitsbewusstsein und der technischen Lösung. Durch die Echtzeitkomponente wird der Benutzer nur mit den Informationsinhalten konfrontiert, die er tatsächlich im Berufsalltag benötigt. Im Rahmen dieses Artikels wird aufgezeigt, wie beide bisher koexistierenden Maßnahmen kosteneffizient zusammengeführt werden können und voneinander profitieren. Ein kurzes Projektbeispiel stellt einen einfachen Fall dar. Der These „Die beste Firewall sind geschulte Mitarbeiter“ steht die Antithese ge-

genüber: „Die notwendige technische Tiefe von Security-Schulungsinhalten für alle Anwender ist in größeren Unternehmen nicht kosteneffizient“. Wie immer liegt die Wahrheit in der Mitte – was auch die Praxis zeigt. Noch kein Unternehmen hat nach der Schulung der Mitarbeiter die Firewall abgeschaltet.

Ist nun der geschulte Mitarbeiter wirklich der beste und kosteneffizienteste Schutzschild? Es steht außer Frage, dass das Know-how der Mitarbeiter ein wesentlicher Faktor für die Produktivität und die



Echtzeit-Awareness am Beispiel der Endpoint-Security-Suite von Itwatch: kein plumpes Verbot am USB-Port, sondern Freiheit bei gleichzeitiger Sicherheit und Compliance

Quelle: Itwatch

Qualität eines Unternehmens ist. Ein Training wird daher auf den konkreten Arbeitsplatz des Mitarbeiters ausgerichtet sein und die qualitativ hochwertige Abwicklung seiner Geschäftsprozesse in möglichst kurzer Zeit adressieren. Trainingsinhalte, die einen Querschnitt aller denkbaren individuellen Fälle bieten, werden dabei von allen Beteiligten als lästig wahrgenommen, da sie ja von der eigentlichen Wertschöpfung – zumindest vordergründig – abhalten.

Die zweifelsohne komplexen Disziplinen Risikomanagement und Sicherheitsmanagement bemühen sich hier im besten Fall zusammen mit dem unternehmerischen Denken der Firmenleitung, den optimalen Wirkungspunkt zu finden.

Viele harte und weiche Faktoren beeinflussen diesen Prozess:

- IT-Wissen und Vorstellungskraft der Mitarbeiter – häufig ist der geringe Verständnisgrad der Mitarbeiter für die „virtuelle Realität“ ein hemmender Faktor bei Security-Awareness-Programmen.
- Wie wichtig ist die Sicherheit der Information für das Unternehmen?
- Welche Risiken sind vollständig oder teilweise bereits durch technische Sicherheitsrichtlinien abgedeckt?
- Ist die Komplexität der Handlungsanweisungen adäquat?

Klar wird hier, dass der optimale Wirkungspunkt immer unternehmensabhängig und in größeren Unternehmen auch je nach Abteilung, Standort oder sogar der jeweils handelnden Person unterschiedlich sein kann. Das macht es natürlich nicht einfacher, die Schulungsinhalte unternehmensweit einheitlich zu gestalten, auf den individuellen Bedarf hin zu optimieren und dabei auch mit der jeweils notwendigen Konsequenz die Schulungsteilnahme einzufordern oder sogar die erlernten Inhalte zu prüfen.

Die Teilnahme an Know-how-Programmen wird in Unternehmen seit langem mit Zertifikaten oder Abschlusstestaten belegt. Nicht jedes Testat weist den Teilnehmer danach als Netzwerkexperten aus, aber auch ein „Datenschutzführerschein“ kann für einen Mitarbeiter, der täglich mit personenbezogenen Daten hantiert, ein wesentliches Qualitätsmerkmal darstellen. Interessant

ist hier zum Beispiel, dass das Bundesdatenschutzgesetz bei der Verarbeitung personenbezogener Daten den mobilen Datenträgern wie Memory Sticks einen besonderen Schutzbedarf zuweist. Für den Vertriebsmitarbeiter einer Versicherung, der die Daten seiner Mandanten zunehmend auf mobilen Datenträgern erhält, liegt hier ein Minenfeld – auch wegen der Haftungsfragen.

Wie immer ist es natürlich besser, diese Awareness-bildende Information zur richtigen Zeit an den „Point of Need“, also den Handlungspunkt zu bringen, als die Richtlinien und Schulungsinhalte in dicken Ordnern verstauben zu lassen. Die Nähe zum Handlungspunkt hat wiederum zwei Facetten: Ort und Zeit. Für den Ort schaffen Online-Awareness-Programme eine gute Akzeptanz, weil sie vom Benutzer an seinem Arbeitsplatz zu einem beliebigen Zeitpunkt – also quasi als Ablenkung vom Tagesgeschäft – durchgeführt werden können.

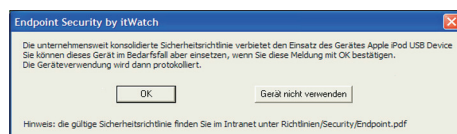
Onlineschulungsinhalte im Intranet sind hier der richtige Weg, da sie kosteneffizient und mit unabhängiger Zeitplanung nutzbar sind. Sofort aber drängen sich ein paar Fragen auf: Haben alle Vertriebsmitarbeiter oder alle Mitarbeiter, die mobile Datenträger einsetzen, die Onlineschulung genutzt und überdies auch verstanden?

Sicherheitssoftware als Assistent

Die Lösung liegt auf der Hand. Wird ein Memory Stick eingesteckt, dann kann man ja den Benutzer in Echtzeit in einem kleinen Dialog fragen: „Haben Sie die Schulung unter www.mycompany.com/IT-Sec/E-Learning/...“ schon absolviert? Bei der ehrlichen Antwort „Nein“ bleibt immer noch die Gelegenheit, bei der nächsten Verwendung des Memory Sticks dringlicher zu werden oder direkt auf die Intranetseite zur Schulung zu verzweigen. Natürlich wird das Unternehmen die Schulungsinhalte nicht nur auf IT-Sicherheit auslegen, sondern auch nützliche Tipps geben und auf häufig begangene Fehler hinweisen. Wer hat nicht schon einmal „schnell“ auf einen Memory Stick Dateien kopiert und sofort nach dem Abziehen festgestellt, dass diese Dateien noch gar nicht „darauf“ sind – in

solchen Fällen empfiehlt es sich das Icon „Sicheres Entfernen von Hardware“ für einen Tipp zum Umgang mit mobilen Datenträgern.

Die Security-Awareness-Gemeinde hat bereits gelernt, dass es eine Sache ist, punktuelle Maßnahmen durchzuführen und eine andere, weitaus schwierigere, ein kontinuierliches Programm zu betreiben, welches alle Interessen über einen langen Zeitraum verfolgt. Betrachten wir dazu die Compliance-Seite, dann sehen wir zwingende



So steigt auch die Akzeptanz: Der Schutzmechanismus assistiert dem Anwender.

Quelle: Itwatch

Gründe für eine Anwendung der Security Awareness in Echtzeit. Der HIPAA-Standard in den USA verlangt unter anderem, dass bestimmte Schulungsinhalte zur Vertraulichkeit von medizinischen Patientendaten in vordefinierten Zeitintervallen zu wiederholen sind – der medizinische Betrieb ist nicht „compliant“, wenn er den entsprechenden Nachweis nicht erbringt. Hier sind natürlich IT-gestützte Prozesse zur Schulung und eben auch zur Verwaltung der Nachweise das Mittel der Wahl. Am besten werden die Rechte digital in Echtzeit an die erfolgreiche Durchführung des Lernprogramms gekoppelt, denn nur dadurch spart man sich administrativen Aufwand, Zeitverzögerungen und Fehladministrationen.

Einige Hersteller von IT-Sicherheitsprodukten haben gelernt, dass das Durchsetzen einer Security-Policy nicht der Weisheit letzter Schluss sein muss, sondern dass gerade bei großen, erfahrenen Kunden die endbenutzerverträglichen Produkte den Vorzug bekommen. Die Anforderung der Skalierbarkeit bekommt hier eine neue Dimension. Die Möglichkeit einer „weichen“ Entscheidung, die abhängig von kundenseitig definierten Vorgaben oder als Reaktion auf Dialoge in Echtzeit zwischen Freigabe und Sperre liegt, wird hier natürlich bevorzugt. Lässt das Sicherheitsprodukt nur eine a priori definierte Entscheidung

zwischen Sperre und Freigabe zu, so kann nicht auf die aktuelle Situation eingegangen werden.

Kein Problem mit Sonderfällen

Besonders positiv ist hier ein Projekt bei einem Mobilfunk-Provider mit etwa 10.000 Arbeitsplätzen aufgefallen, in welchem gleich mehrere der oben angesprochenen Facetten zusammenkommen. Dort wurde flächendeckend eine flexible Endpoint-Security-Lösung implementiert, um konsolidierte Sicherheitsrichtlinien durchzusetzen. Natürlich sind Ausnahmen von der allgemeinen Richtlinie für Manager, VIPs, Administratoren und andere Benutzer je nach deren IT-Kennntnis und Tätigkeitsfeld notwendig. Die Ausnahmen könnte man natürlich einfach in die technischen Regelungsmechanismen einbauen. Gewählt wurde in der Installation aber ein Weg, der von einem besonderen Feature des gewählten Produkts Gebrauch macht: der Möglichkeit zur Änderung der Sicherheits-Policy in Echtzeit – abhängig vom Systemzustand oder sogar von interaktiv erzielten Ergebnissen. Statt Freigaben für die Benutzer fest einzutragen, ist ein Dialog implementiert: „Die unternehmensweit konsolidierte Sicherheitsrichtlinie verbietet den Einsatz des Geräts ... Sie können dieses Gerät im Bedarfsfall aber einsetzen, wenn Sie diese Meldung mit OK bestätigen. Die Geräteverwendung wird dann protokolliert.“ Dieser Dialog schafft Security Awareness in Echtzeit, erstellt geeignete Log-Einträge für den Auditor oder die Revision und fordert gleichzeitig die aktive Benutzerzustimmung ab. Es kann ein beliebiger kundenseitig definierbarer Algorithmus eingehängt werden, sodass sich die Nutzung eines Geräts oder die Erlaubnis zum Kopieren einer sensiblen Datei auch vom Schulungsstatus oder anderen Eigenschaften des Nutzers oder des Rechners abhängig machen lassen. Dies ist eine erfreuliche Entwicklung, da die bisher unterschiedlichen Welten „Security Awareness“ und „Security Policy Enforcement“ (Durchsetzung von Sicherheitsrichtlinien) elegant miteinander kombiniert werden können.

Irmgard Bähr/wj