AwareWatch

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 München

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

www.itWatch.de
info@itWatch.de

AwareWatch

Granulare Security Awareness im Handlungskontext – praktisch und kosteneffizient

- **Der Mitarbeiter als integraler Bestandteil der IT-Sicherheit**
- **„Darf ich oder darf ich nicht? Wie geht das sicher?" Eine Entscheidungshilfe im Dialog**
- **Compliant handeln - Wie geht das?**
- **IT-Sicherheit muß nicht verhinderen sondern kann das richtige Handeln befördern**
- **Minimalinvasive Sicherheit**

Nicht jeder Mitarbeiter kann auf jede kritische Situation innerhalb der Verwendung seiner IT geschult werden – hauptsächlich weil er nicht alle kritischen Aktionen erkennen kann. Der Mitarbeiter merkt nicht, wenn über Bluetooth eine Geräteinstallation auf dem Client initiiert wird oder der Browser durch eine Drive-by-Attacke eine DLL oder ein Executable modifiziert. Mitarbeiter und die „Business-Owner" sind unzufrieden, wenn prophylaktisch alles verboten ist und sie durch „die (überzogene) Sicherheit" in Ihrer Entscheidungsfreiheit und Produktivität eingeschränkt sind. Security Awareness in Echtzeit bindet den Mitarbeiter in die IT-Security des Unternehmens ein und schafft die Freiräume, die der Mitarbeiter und das Business brauchen.

Mit **AwareWatch** tritt der Sicherheitsverantwortliche automatisiert direkt am Ort des Geschehens zum Zeitpunkt der kritischen Aktion in Dialog mit dem Anwender und zwar in Echtzeit. Er entwickelt im Unternehmen eine Sicherheitskultur und kann diese in einfacher Weise mit zentral definierten Maßnahmen aktuell halten.

Compliance heißt zunehmend, dass das rechtssichere Handeln aller Anwender gegenüber einem Auditor jederzeit durch revisionssichere Unterlagen nachgewiesen werden kann. Technisch kann das z.B. durch eine nach deutschem Gesetz gültige elektronische Willenserklärung, die einen juristisch gültigen Vertrag in Echtzeit darstellt, umgesetzt werden.

Die Benutzer fühlen sich durch die direkte Ansprache mit Dialogen und Auswahlmöglichkeiten nicht gegängelt. Selbstfreigabe mit der Auflage der Protokollierung senkt die administrativen Kosten und erfüllt die Wünsche der Nutzer, der Business Owner UND der Unternehmensführung.
Durch die Auslagerung von kritischen Aktionen in ReCAppS Umgebungen kann der Anwender alle Aktionen eigenständig ausführen, ohne die Sicherheit zu gefährden. Die IT-Sicherheit wird dadurch zum Business-Enabler und gilt nicht mehr als Verhinderer von Geschäft.

Spontane Rechte mit Projektbezug: Der Benutzer kann durch Eingabe eines gültigen Projektnamens aus einem vordefinierten Pulldown Menü oder im Freitext seine Rechte, wie in der zentralen Sicherheitsrichtlinie definiert, erweitern und die Objektzuordnung zu dem Projekt klarstellen. Jede Aktion unterliegt dann der vorab definierten Geräte- und Inhaltskontrolle. Im Außendienst kann z.B. der Kunde oder das betroffene Objekt über den Dialog eingegeben und revisionssicher hinterlegt werden.

Situationsabhängige Kontrolle: Die Freigabe der kritischen Aktion kann zeitlich gesteuert werden. Sofortige Freigabe ist ebenso möglich wie Herauszögerung, damit der Benutzer zuerst die Compliance-Informationen gelesen und dieser zugestimmt hat, bevor beispielsweise ein Massenspeicher eingesetzt werden darf.

Häufigkeit der Aktion definieren: Je Benutzer oder PC kann die Häufigkeit der Aktion nach algorithmischen Parametern frei definiert werden. Für eine automatische und beweissicher gespeicherte vierteljährliche Belehrung, wie z.B. in HIPAA gefordert, kann der gesamte Prozess technisch beweisbar abgedeckt werden.

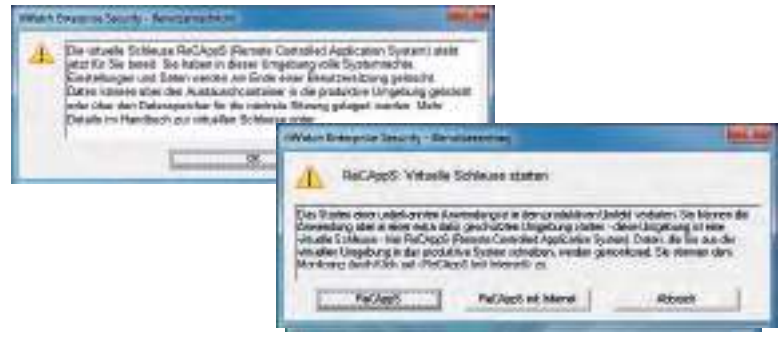
Echtzeitmonitoring: Der vom Benutzer eingegebene Text erscheint im zentralen Logging des Echtzeitmonitors der itWatch und kann inhaltsabhängig im Echtzeit in der itWESS oder über Drittprodukte eskaliert werden.

Frei definierbare Dialoge: Die Endbenutzer-Dialoge können bequem und flexibel kundenseitig angepasst werden. Eine Einbindung in die Corporate Identity (Firmenlogo im Dialog) erzielt hohe Akzeptanz beim User und unterscheidet die Dialoge von typischen Meldungen des Betriebssystems.

Einbringen von Plug-Ins: Ohne Zutun des Herstellers kann der IT-Verantwortliche einen eigenen Algorithmus als Plug-In einbringen und diesen vor, während oder nach einer spontanen Freigabe zur Prüfung oder zum Alerting einhängen.

Nutzungsbeispiel:

- In einer Word-Datei ist ein ausführbares Programm eingebettet
- Die Datei darf daher nicht auf den Rechner kopiert werden
- Öffnen der Word-Datei in einer geschützen Umgebung (ReCAppS) ist möglich und wird technisch erzwungen
- Der Anwender kann entscheiden, ob er dafür Internetzugang benötigt oder nicht.



FSAW-190327