WISSEN SCHÜTZT VOR DATENKLAU

LNK-Dateien mit Schadfunktion, Spyware in PDF-Dateien: kein Anwender kann „Zero-Day-Exploits“ erkennen! Dienstvereinbarungen haben an dieser Stelle ausgedient. Trotzdem gewinnt „Security Awareness“ für Unternehmen immer mehr an Bedeutung. Denn nur mit technischem Schutz UND der Zusammenarbeit mit dem geschulten Anwender kann man den immer komplexeren Angriffen begegnen. Die Presse ist reichlich gefüllt mit Meldungen über Datenklau, Computerspionage und Angriffen auf Unternehmen. Rechtlich wird gerade die Haftungsfrage in neue Dimensionen getrieben, indem z.B. Steuersünder bei den verantwortlichen Banken ihren zusätzlichen Schaden einklagen.

Im Idealfall wird der Anwender in Echtzeit auf die Risiken seines Handelns, die geltenden Richtlinien und Möglichkeiten sicherer Handlungsalternativen aufmerksam gemacht, technisch überwacht und bei Bedarf vor notwendigen, kritischen Aktionen online geschult. Zusätzlich gilt die Zustimmung des Benutzers, revisionssicher gespeichert, als elektronische Willenserklärung.

Der Schutz der Unternehmensdaten kann durch verschiedene Verfahren umgesetzt werden. Entweder durch proaktiven Schutz mit Verboten, durch Beweissicherung und damit verbundener Haftung, organisatorische Vereinbarungen, die am besten in Echtzeit revisionssicher geschlossen werden oder bewusstseinsverbessernde Maßnahmen (Security Awareness). In der Praxis ist eine Kombination der genannten Möglichkeiten der beste Weg, um die jeweilige Lösung an die Anforderungen von einzelnen Benutzergruppen, Standorten oder Unternehmenseinheiten anzupassen. So kann man jeweils die Stärke des Schutzmechanismus, die gewünschte Sicherheitskultur des Unternehmens und die Freiräume einzelner Anwendergruppen ohne Eingriffe in die Unternehmensabläufe individuell anpassen. IT-Sicherheit wird dann nicht als Verhinderer wahrgenommen. Die stete Veränderung der Rechtslage und der Regularien erfordert Dynamik: eine flexible, zentrale Administration mit schnellen Reaktionsmöglichkeiten ist gefragt. Kostenreduktion in den Help Desk Prozessen und unterbrechungsfreier Einsatz von Notebooks im Hausnetz, unterwegs und am Heimarbeitsplatz erfordern dynamische Security Policies, die sich sogar in Echtzeit den Bedürfnissen Ihres Unternehmens anpassen müssen.

Wissen schützt vor Datenklau

Die itWatch Endpoint Security Suite bietet Ihrem Unternehmen die geforderte Flexibilität und die nötige technische Sicherheit als Schutz vor Spyware, Malware, malicious Code und vielen weiteren Angriffen, die das Wissen des Anwenders überfordern. Themen wie Zustimmungspflicht, Kenntnisstand des Mitarbeiters, Zustimmung des Nutzers zur Protokollierung, Nachweis über den Projektbezug einer kritischen Tätigkeit, etc. bestimmen nach zentralen Richtlinien in Echtzeit am Ort des Geschehens die Möglichkeiten und Handlungsauflagen.

So werden verschiedene Welten für den Kunden gewinnbringend zusammengeführt:

1. Das Wissen des Endanwenders um die Sensitivität einer Datei.
2. Das Wissen der zentralen IT um aktuelle Angriffe, technische Zusammenhänge, Richtlinien, die technische Sicherheit von Datenträgern und Prozessen sowie die Verlässlichkeit von bestimmten Benutzergruppen und eigenverantwortlich handelnden Mitarbeitern.
3. Die Investitionen in Security Awareness-Maßnahmen kommen in Echtzeit an den Nutzungspunkt.
4. Die intern geklärte Haftungsfrage und Haftungsübergänge.
5. Technisch umgesetzte Compliance-Anforderungen, die mit zentral definierter Information in Echtzeit mit dem Benutzer kommuniziert, revisionssicher abgelegt wird und dadurch beweisbare Compliance auf Knopfdruck leistet.

Die Endpoint Security Suite bietet folgende Funktionen:

- **Device- und Port-Kontrolle** – Wer darf welches Device wann und wo in welcher Situation nutzen? Für neue Geräteklassen oder Ports darf kein Update nötig werden.

- **Content-Kontrolle** – Für den Lesezugriff freigegebene Daten dürfen keinen Schadcode enthalten (LNK, PDF, verschlüsselte ZIP-Archive...). Firmenvertrauliche Daten dürfen nicht mitgenommen werden.

- **Dialog, Protokollierung und Alerting** – Compliance erfordert Beweisbarkeit. Bei freigegebenen, sicherheitskritischen Aktionen ist deshalb neben dem Alerting die Möglichkeit zur Protokollierung ein Muss. Ein Filterverfahren vermeidet Datenflut. Der Kunde definiert, welche sicherheitskritische Aktion einen Echtzeitdialog mit dem Anwender erfordert: z.B. Selbstfreigabe, Datenschutz, Nutzung kritischer Daten, Netzwerke, Hardware oder Anwendungen.

- **Benchmark des Risikos** – Die Protokollierung definiert die aktuelle Risikosituation und ermöglicht es, die Risiken anonym oder pseudonym in Qualität und Quantität direkt in das Risiko-Management zu übergeben.

Wissen schützt vor Datenklau

- **Verschlüsselung sensibler Information** – Nachteil der Partitions-verschlüsselung ist, dass ein einziger Schlüssel große Datenbereiche transparent frei gibt. Moderne Verfahren sind mit Unternehmensschlüsseln und privaten Schlüsseln ausgestattet, die je nach Berechtigung des Anwenders und der Sensitivität der Daten zu einer optionalen oder zwangsweisen Verschlüsselung der Inhalte führen. Die zwangsweise Verschlüsselung mit einem Firmenschlüssel reduziert das Risiko des Datendiebstahls auf null Prozent.

- **Kontrolle der Anwendungen** – Überblick schafft das Monitoring aller Anwendungen mit ihren authentischen Merkmalen. Freigabe und Sperre erfordern aus praktischen Gründen White Lists UND Black Lists – dabei sind situationsspezifische Freigaben erforderlich. Die Kontrolle der Dateizugriffe von Anwendungen schützt vor Spyware, macht Legacy-Anwendungen sicher und erlaubt den geschützten Betrieb unsicherer Anwendungen in „Sandboxes“.

- **Kontrolle der verwendeten Netze** – Die Netzwerk-, UMTS-Karten, WLAN-Geräte usw. verbinden den Rechner mit potentiell gefährdeten Netzen. Entsprechend des erkannten Netzes wird die Security Policy in Echtzeit eingestellt (Heimarbeitsplatz, Firmenzentrale, etc.).

- **Personalisierung von Datenträgern** – In kritischen Bereichen müssen wesentliche Datenbewegungen beweisbar abgelegt werden. Den „unternehmenseigenen Datenträger“ erstellt man durch Personalisierung auf die Gruppe der Domänenbenutzer mit zwei Mausklicks und vermeidet damit aufwändige Verfahren und den Einkauf teurer Hardware.

- **Security Awareness in Echtzeit** – Schulungsinhalte, die nicht täglich angewendet werden, vergisst man. Die Lösung: Lerninhalte und die Zustimmung zur Protokollierung direkt an die kritische Aktion koppeln.

- **Lokale Schleusenfunktion** – Entschlüsselung und Dekomprimierung in einer lokalen Quarantäne – erst dann können die Inhalte im Klartext geprüft werden. Je nach Ergebnis, werden die Dateien geblockt und sicher gelöscht, zur Prüfung an Dritte weitergeleitet oder freigegeben – zusätzliche Hardware und lange Wege sind unnötig.

Für weitere Informationen kontaktieren Sie uns unter:

Info@itWatch.de oder 089/ 620 30 100.

itWatch GmbH
Aschauer Str. 30
D-81549 München