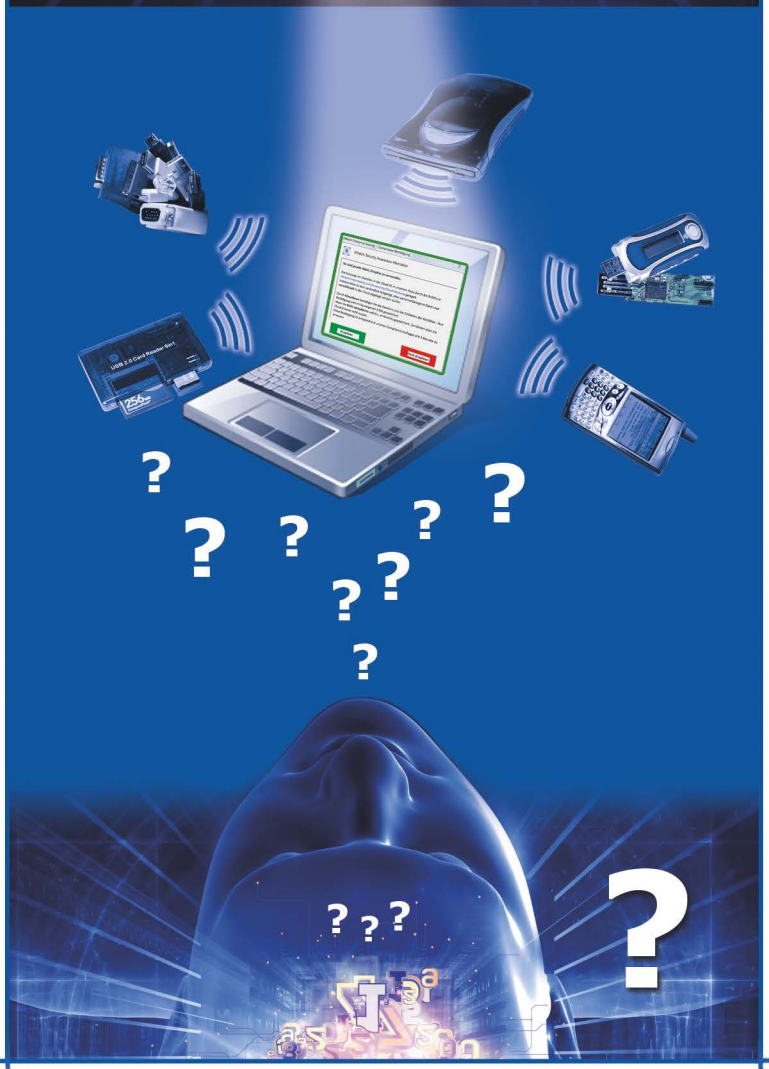
AwareWatch



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 in context of action – practical and cost-effective

- The employee as an integral component of IT-Security
- „May I or may I not? How does it work secure?" decision support in dialogue
- Compliant acting – How does it work?
- IT-Security don´t have to prevent but can stimulate right acting
- Minimal invasive security

The employee as an integral component of IT-Security

Not every employee can be instructed for every critical situation within the use of his IT – mainly because he cannot identify every critical action. The employee don´t notice, when a device is being installed over bluetooth on the client side or the browser is getting modified by a Drive-by-Attack, a DLL or an executable. Employees and the „business-owner" are discontented, if everything is forbidden prophylactically and their autonomy of decision as well as productivity are restricted due to „the (exorbitant) security". Security Awareness in real time connects the employee with the corporate IT-Security as well as creates open space, which is needed by employees and business.

May I or may I not?

AwareWatch creates a dialogue in real time between the security officer and the user - automatically direct at the scene of the event during the time of the critical action. He develops a security culture in the company and can keep it up to date in a simple way with central defined policies.

Compliant acting

Compliance means increasingly to enable the evidence of the legally secure acting of all users to an auditor anytime through auditable data. Technically it can be realised e.g. through an electronic declaration of intent valid according to German law which constitute a legally valid contract in real time.

Stimulating right acting

Because of the direct attention with dialogues and options the users don´t feel overlooked. Autonomous approval with the restraint of logging declines the administrative costs and fulfils the desires of the users, the business owner AND the management. Through the outsourcing of critical actions in ReCAppS environments the user can realise autonomously every action without putting the security at risk. Thus the IT-Security becomes the business-enabler and isn´t seen as a preventer of business.

May I or may I not?

Spontaneous rights related to projects: The user can expand his rights by entering a valid project name out of a predefined pulldown menu or as free text as defined in the central security policy and can clarify the object assignment to the project. Every action is subjected to the predefined device and content control. In the field e.g. the costumer or the affected object can be entered via dialogue and deposited auditable.

Situation-dependent control: The approval of the critical action can be controlled temporarily. Immediate approval is possible just as postponement so that the user read and agree at first the compliance information before e.g. the mass storage can be used.

Defining frequency of actions: For each user the frequency of the actions can be defined freely according to algorithmic parameters. The whole process can be realised technically provable for an automatically and evidentially saved quarterly instruction as e.g. demanded in HIPAA.

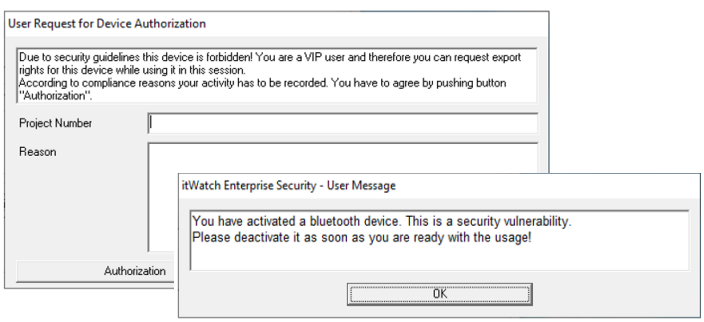
Real time monitoring: The text entered by the user appears in the central logging of the real time monitor of itWatch and can be escalated depending on the content in real time in itWESS or through third party products.

Free definable dialogue: The end user dialogues can be adjusted at ease and flexible on the part of costumer. An Integration in the corporate identity (company logo in the dialogue) achieves high acceptance from the user and differentiate between the dialogues and typical operating system messages.

Inserting Plug-Ins: The IT-Security officer can insert an own algorithm as Plug-In without help of the producer. He can insert the algorithm before, during or after a spontaneous approval for examination or alerting.

Examples for use:

- An executable program is inserted into a Word document
- Copying the data file is not allowed on the computer
- Opening the Word file in a protected environment (ReCAppS) is possible and is technically enforced
- The user can decide whether he need access to the internet or not



FSAW-200408