DLP Best Practice
Quick Wins
- Sustained Risk Reduction

Like any other property, data must be protected against unauthorized withdrawal and theft – that's common understanding. But what is the best way to do that? How is it possible to achieve verifiable success in the shortest time, and how can hidden pitfalls in DLP (Data Leakage Prevention) projects be avoided?

Identify criticality

A bit doesn't show, whether it is confidential, encrypted or public. A confidential content is still confidential even as a printout, part of an archive (i.e. zip file), copy of a screen, encrypted e-mail attachment or embedded in a PowerPoint file. Representations of the text, like ü (u umlaut)/ue, capital letters, 8-bit/16-bit representation, ASCII, DOS, EBCDIC and many more variants can complicate the recognition. Moreover, a certain fuzziness is inherent to any fully automated process of labeling according to the criticality (public, confidential etc.) of the data in cause.

Checkup of permissions

For a proper decision in real time it is essential to have information on the context the current action takes place in. It's perfectly ok, on a DVD to store local data, which is encrypted with an enterprise key exclusively used inside the company, but the withdrawal of the same data with a transport key by a trainee is to be prohibited. Hence, the effective decision will always be depending on the situation, but still it has to be fixed proactively in the security policy in effect.

Avoiding pitfalls

The most common mistakes in DLP projects:
1. Companies at first trying to mark all the existing data according to their criticality, will waste much time and energy, and will be waiting for a long time for the expected positive results. The real goal, that is to protect data against unauthorized withdrawal, will never be achieved.
2. Ignoring the inaccuracies caused by the system during the classification will result in a lot of false positives and false negatives, and as a consequence many subsequent improvements during operation will be required, generating high administrative costs. The alternative, setting real protection criteria very low, is not a viable option either – the results wouldn't be worth the effort. Thus, over time the increasing annoyance with the system's inherent inaccuracies can damage the whole project

3. Focusing solely on the data withdrawal, could obstruct the view on attacks from outside the company, which eventually result in unwanted data withdrawal. In many cases in the first place the attacks of standard applications (Internet Explorer exploits) or those on standard formats (PDF-Exploits) are opening outbound data channels. However, as the attack comes from outside the company, it is one of the mission critical tasks for DLP to control or prohibit "the import of detrimental executable objects" like Java scripts in PDF, the DLL download via browser etc.

Best Practice Stage 1

Quick wins are important at the beginning of a project. They are achieved by simple, for the operation uncritical security measures. The potential leakage points are quickly identified: contact points in the net and local ones over cable or wireless (Bluetooth, WLAN etc.), communication applications (E-mail, browser etc.) and mobile devices. In a first step, security measures should be chosen in a way as not to interfere with operations. This kind of measures, like creating security awareness, monitoring and alerting, allow for a repetitive refinement of the criticality estimations. A periodic checkup of the statistical analysis shows on the one hand the real risks and on the other hand the actual breaches of existing policies. After this first steps, which can be done within a few hours, there are already clear answers available to the question: "How secure are we?".

Best Practice - Further steps

The activities in stage 1 set the foundation for the continuous refinement of the technical security measures like blocking and mandatory encryption, which only in stage 2 translate into the proper case specific measure. Depending on the application, network, the active users and of course the identified data content the following actions can be enforced: encryption with an enterprise key or personal key, awareness or knowledge information for users in real time on the identified risk, electronic declaration of intent of the liability transfer, audit-prove taking of evidence or blockade. When choosing a technical product, one of the essential criteria should be the possibility to integrate the product's own algorithmic checkups as well as those from third party programs, in order to create a sequence of interdependent checkups on different criteria. In the medium term the most sensitive data should be stored in separate subnets (Read up – No write down) and these subnets should be integrated exclusively via virtual mechanism.

Conclusion

By choosing the right solution, even for the complex area of DLP the protection of investment, scalability, sustainability and operational cost efficiency can be combined with a quick success in a project. The best way to achieve this consists in choosing the support by a technical tool, that provides risk management and the protection features in one single product and thus being able to completely represent the life cycles of risks and data.

Contact

info@itWatch.de for product information,
PR@itWatch.de for press,

itWatch GmbH
Aschauer Str. 30
D-81549 Munich

Call +49 89 620 30 100
For further information **please visit**:
www.itWatch.info