Protecting what matters for your business

Assess your security readiness to protect your assets from next generation attacks

The value of information owned by and about your company can be demonstrated by the never ending news on Wikileaks, un-detected cyber-attacks from competitors and data losses due to staff behavior. Most of these issues involve the technology aspect and to a large extent, the human factor. But how can you protect your company's valuable assets against the unknown?

Industry espionage for everyone

The increased professionalism and organization of attackers has moved the goal-posts. The motivation of today's attacks goes beyond the technical kick and has a profound criminal, political or military background. The combination of the availability and affordability of commercial hacker tools, with an increasing connected and therefore remotely vulnerable world, results in a new paradigm:

Espionage has become part of global competition, for example:

- Google disclosed a highly sophisticated cyber-attack from China resulting in the theft of IP data
- Starwood sued Hilton over trade secrets where two former Starwood executives stole secret data

The easiest path is taken first

Sophisticated attackers choose their attack method carefully and these are becoming increasingly more social (the "human factor"). The "right" question from a falsely trusted person might reveal a password or an unsecured window, which could allow an attacker to decode data via access to the hardware. Corporate safety relies on the weakest link and only a 360-degree view will help you identify and mitigate the risk. Protecting your business effectively requires a holistic approach that focusses on important integrated layers.

The principle security layers are strategy, culture and processes, as well as the technology itself. Each individual data protection and disaster management, continuous risk, auditing and change management. To protect your business, the security concept needs to address each integrated security layer and respective domains accordingly.

Better than industry average

Today, with widely available knowledge and technology, there is no absolute security because it is only a matter of resources to overcome any security barrier. Therefore your objective is to ensure that your security level is high enough to distract hackers from targeting your company.

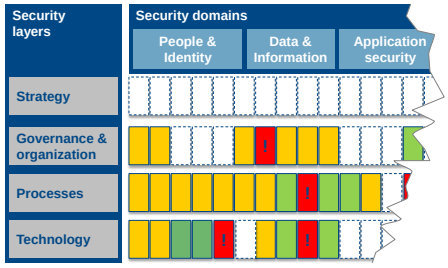
Internally, your company must be aware of where most security breaches occur and there should be no un-controlled temptations. It is not sufficient to have an annual review that reveals unauthorized access but instead to establish a culture and daily processes that prevents security breaches from very beginning.

Externally, your company needs to be better protected than other comparable targets. Put yourself in the hacker's shoes: why take the extra effort to invade the better protected target? You need to be "just slightly" more protected than any of your neighbors in terms of industry, geography and technology.

This also implies an early-mover advantage. If you are fixing security holes faster than others, you are unlikely to be the first target of potential attackers. Furthermore your investments and implementation risks will be less compared to your competitors who are adapting more slowly.

Security health check

Perception and reality are far apart in the arena of security. Often the classical IT function cannot reach beyond infrastructure, and corporate security can miss the required technological skills. The key success factor is to have transparency: know your vulnerabilities, the attractiveness for attackers and the value at risk. To get a clear and neutral picture, a third-party 360 degree assessment is necessary. As a starting point we recommend a holistic security health check through all security layers and through all relevant domains. From this we can identify the weak aspects of your system in comparison to state-of-the art protection, going beyond falsely trusted compliance and legal regulations.



On the basis of this scan, clear imperatives can be derived such as closing technical security gaps, raising employee awareness and setting up crises intervention teams for severe incidents.

Arthur D. Little has compiled an expertise-based toolset to assess maturity, capability and security strategy of corporations – an approach to efficiently and effectively identify, and close weak points. We use the results of the assessment as the starting point to craft a holistic security concept to protect what matters for your business.

Contact:

Dr. Fabian Dömer
Managing Director
+49 (0) 69 450098 100
doemer.fabian@adlittle.com