

Sicurezza logica

Logical Security

The context

Security management is a strategic point for companies. As a matter of fact, data protection and IT business continuity represent a key issue for the whole business. In a world where IT attacks are always more sophisticated and exploit all possible vulnerabilities in information infrastructures, applications, processes and human behaviours, it is of paramount importance to cope with the problem in a comprehensive way, guided by partners who can support companies in terms of experience, competences and continuous update.

The Akhela solution

The Akhela solution is comprised of a suite of autonomous modules which are integrated in a continuous process which allows each company to manage its IT security needs in the best way. Each module is the result of specific experiences and is continuously updated to cope with the new threats that are launched on a daily basis against business security. A steady monitoring of the international market allows to integrate the home developed solutions with the most reliable and technologically advanced products. Akhela's activities aim at the management of complex data center, networks of any dimension and protocols, multiplatform systems, active directories and complex e-mail systems. Akhela has adopted innovative solutions for wireless security, application security and social engineering.

The process

Assessment

The aim is to identify the critical points and the formulation of the vulnerability assessment.

- Vulnerability Assessment & Penetration Test: check of the existing vulnerabilities through the IT infrastructure analysis and attack simulations carried out also with ethical hacking methodologies.
- Risk Analysis: spotting and evaluation of the architectural vulnerabilities and resulting risks; setting out the action's priorities.

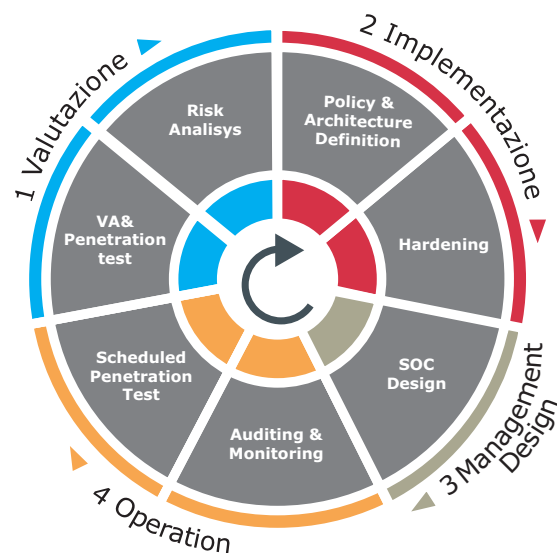
Il contesto

La gestione della sicurezza è un fattore strategico per le aziende. La protezione dei dati e la garanzia della continuità dei sistemi informativi sono infatti una condizione irrinunciabile per il business. In un contesto di attacchi informatici sempre più sofisticati che sfruttano ogni possibile vulnerabilità, dall'infrastruttura informativa alle applicazioni, dai processi alle prassi comportamentali, è ormai necessario affrontare il problema in modo diretto e strutturato, affiancando alle proprie competenze partner che sappiano dare un valore aggiunto in termini di esperienza, competenza e aggiornamento continuo.

La soluzione Akhela

La soluzione di Akhela è costituita da una suite di moduli autonomi ma integrati in un processo continuo che consente di gestire in modo coordinato le esigenze di sicurezza di ogni Azienda. Ogni modulo nasce da esperienze specifiche e viene costantemente aggiornato a fronte delle nuove sfide che quotidianamente vengono lanciate alla sicurezza aziendale. Un costante monitoraggio del mercato internazionale consente di integrare le soluzioni sviluppate internamente con i prodotti tecnologicamente più avanzati e affidabili.

L'intervento di Akhela è mirato alla gestione della sicurezza di data center complessi, network di qualunque dimensione e protocollo, sistemi multiplatforma, active directory, sistemi complessi di posta elettronica. Akhela ha adottato soluzioni particolarmente innovative nell'area della sicurezza wireless, dell'Application Security e del "social engineering".



Le fasi del processo

Fase di valutazione

L'obiettivo è l'individuazione dei punti critici e la formulazione dell'assessment delle vulnerabilità.

Vulnerability Assessment & Penetration Test: verifica delle vulnerabilità presenti, attraverso l'analisi dell'infrastruttura ICT e mediante simulazioni di attacchi svolte anche con i metodi di ethical hacking.

Risk Analysis: individuazione e valutazione delle vulnerabilità architetturali e dei rischi che ne derivano; definizione delle priorità di intervento.

Sicurezza logica

Implementation

The aim is to set up the security policies and the subsequent infrastructure adjustment.

- Policy & Architecture definition: policy, processes and architectures reshape in order to reach the required security level. Check of the policy utilization.
- Hardening: securization of the components and the relevant management processes. Customized operational guidelines for secure installation and configuration of particular systems and networks.

Design management

Planning and implementation of security management system. In particular, in case of SOC (Security Operation Centre) design, the fulfilment of an integrated system of architectures, tools and processes is foreseen, with the aim to guarantee the requested security levels.

Management

Continuous management of security according to shared best practices.

- Auditing & Monitoring: management, on a regular basis, of infrastructure security according to agreed upon forms, through the implementation of procedures, tools and periodical assessments.
- Scheduled penetration test: periodical assessment of the IT infrastructure in order to point out possible vulnerabilities.

Business Partner

In order to carry out some of the above mentioned steps, Akhela utilizes products and technologies of partners who have distinguished themselves worldwide as leaders in innovation and reliability. The following is a list of these products:

- AVDS
- Endpoint Access Manager
- Intellinx
- Network Vault
- Spy Sweeper
- View Suite

akhela

Sesta Strada Ovest - Z.I. Macchiareddu
I-09010 Uta (CA)
Tel. 070/24661000
Fax 070/24661111

Via Larga, 13
I-20122 Milano
Tel. 02/7737472
Fax 02/7737449

Viale dell'Esperanto, 71
I-00144 Roma
Tel. 06/54210205
Fax 06/5912826

Centro Piero della Francesca, C.so Svizzera, 185 bis
I - 10149 Torino
Tel. 011/7750901
Fax 011/775710

www.akhela.com
info@akhela.com

Fase di implementazione

L'obiettivo è la definizione delle policy di sicurezza e il successivo adeguamento dell'infrastruttura.

Policy & Architecture definition: rivisitazione e ridisegno delle politiche, dei processi e delle architetture con l'obiettivo di ottenere i livelli di sicurezza richiesti. Check dell'applicazione delle policy.

Hardening: securizzazione delle componenti e dei relativi processi di gestione; redazione di guide operative customizzate per installazioni e configurazioni in sicurezza di particolari sistemi e network.

Fase di management design

Questa fase prevede la progettazione e realizzazione del sistema di gestione della sicurezza. In particolare, nel caso del SOC (Security Operation Centre) design, è prevista la realizzazione di un sistema integrato di architetture, strumenti e processi in grado di garantire nel tempo, e al variare delle condizioni, i livelli di sicurezza

Fase di gestione

L'obiettivo è la gestione continua della sicurezza secondo best practice condivise.

Auditing & Monitoring: gestione in maniera continuativa della sicurezza delle infrastrutture secondo modalità concordate, attraverso l'implementazione di procedure, strumenti e verifiche periodiche.

Scheduled penetration test: verifiche periodiche dell'infrastruttura ICT per evidenziare eventuali vulnerabilità.

Business partner

Per svolgere alcune fasi del processo, Akhela utilizza i prodotti e le tecnologie di alcune aziende partner che si sono distinte nel panorama internazionale per innovatività ed affidabilità. Di seguito si elencano questi prodotti:

- AVDS
- Endpoint Access Manager
- Intellinx
- Network Vault
- Spy Sweeper
- View Suite