]HackingTeam[

Company profile

Company overview

Sicurezza Informatica (difensiva ed offensiva)

Vendor Independent

Fondata nel 2003

2 soci fondatori e Amministratori operativi

Finanziata da 2 primari fondi di Venture Capital

Fatturato 2011: € 6* mln

Organico: 35

www.hackingteam.com

*stimato

]HackingTeam[

Alcuni clienti

Alcuni clienti

Alcuni clienti

]HackingTeam[

Attività e soluzioni offerte

Ethical Hacking

Protezione del patrimonio informativo

Controllo Accessi

Virtualizzazione sicura delle applicazioni

Gestione password amministrative e gestione privilegi utente

Accesso sicuro alla rete

Next Generation Enterprise WIFI

Governo del rischio

Sicurezza Applicativa

Database Activity Monitor

Mobile Device Management

Rilevamento Anomalie

Gestione dei Log

Attività investigative

]HackingTeam[

Ethical Hacking

- Penetration test del perimetro interno ed esterno
- Simulazione profilo tipo (utente/consulente/fornitore)
- Web application hacking & code review
- Security assessment Wireless
- Security assessment Database
- Security assessment ESX VMWARE
- Security assessment sistemi VOIP
- Security assessment SAP

Protezione del patrimonio informativo

DLP (Data Loss Prevention & IRM)

Meccanismi di controllo tecnologici e organizzativi volti individuare e prevenire la trasmissione e la dispersione di informazioni riservate dal sistema informativo di un'organizzazione verso il mondo esterno (rilevamento anomalie comportamentali, tracciamento attività, classificazione delle informazioni, protezione proprietà intellettuali, ...).

BOOLE™ server

]HackingTeam[

Controllo accessi

Insieme di politiche, processi, procedure e tecnologie volte ad aiutare un'organizzazione nella gestione degli accessi alle informazioni (SSO, autenticazione forte "MULTIFACTOR", autenticazione forte tokenless, on demand token...).

]HackingTeam[

Virtualizzazione delle applicazioni

Soluzione che consente a più applicazioni di essere virtualizzate insieme per creare uno spazio di lavoro virtuale sicuro che separa le impostazioni, le applicazioni e i dati dal sistema operativo, permettendo loro di interagire. Tutto gestito in modalita' centralizzata.

]HackingTeam[

Gestione delle password amministrative e dei privilegi utente

- PBWD: sistema per la gestione degli utenti amministrativi locali (windows).
- Estensione dei privilegi di base ai “normal user” su base nominale
- Integrazione “soft” con AD e configurazione basata su GPO
- Password Safe: Gestione delle password centralizzate condivise
- Integrazione con LDAP
- Profilazione & Audit

beyondtrust
privilege. made simple

]HackingTeam[

Accesso sicuro alla rete

Network Access Control - Forescout

Gestione sia con protocollo 802.1x che SNMP per cui completamente integrabile nell'infrastruttura esistente, inoltre e' "agentless" per verificare la compliance di un device che si collega alla rete. Permette inoltre di identificare i dispositvi come smartphone, tablet in modalita' agentless.

Next Generation WIFI

WIFI 2.0 - Aerohive

Aerohive e' una soluzione per l'implemetazione di una infrastruttua WIFI in ambiente corporate. Le pricipali caratteristiche sono la assoluta mancanza del concetto di controller, ogni AP e' dotato di FW, IPS e QoS, identifica i "*rogue access point*" e' possibile implementare PSK / Policy per utente e dispositivo e molto altro ancora. Il sistema di gestione puo' essere virtuale, applicance fisico o cloud based.

]HackingTeam[

Governo del rischio

Servizi mirati alla formalizzazione di politiche per la protezione delle informazioni, linee guida e standard la cui applicazione è garantita da procedure operative al fine di tutelare gli obiettivi, le missioni e il patrimonio informativo dell'organizzazione (ISO 27001, NIST SP 800-30)

Governo dei dati non strutturati

politiche e tecnologie volte all'individuazione di "*chi accede a cosa e quando*" in termini di visibilita', controllo, audit e reportistica

BLACKBIRD™ GROUP

varonis

]HackingTeam[

Accesso remoto sicuro

E’ una connessione cifrata che garantisce la riservatezza dei dati all’interno del canale tramite client come PC, smartphone e tablet. Oltre a garantire la riservatezza nella comunicazione e’ possibile introdurre meccanismi di One Time Password, Single Sign On sia sul PC che sullo smartphone o tablet utilizzato. In quest’ultimo caso e’ possibile utilizzare direttamente sui device mobili delle “APP” che generano chiavi di accesso “one time”.

Sicurezza applicativa

Meccanismi di controllo tecnologici e organizzativi volti a prevenire violazioni nelle policy di sicurezza di un'applicazione o del sistema operativo e causate da difetti nella progettazione, nello sviluppo e/o nella messa in produzione (protezione applicativi web, analisi applicativi proprietari, disponibilità dei servizi,...).

Database Activity Monitor

McAfee DAM è costituito dalla soluzione Hedgehog Enterprise: si tratta di una soluzione non invasiva (read-only, nessun reboot del server, nessun restart del/dei database), che controlla tutte le attività legate all'uso di un database (DAM - database activity monitoring), ed intempo reale è in grado di prevenire tentativi di intrusione, proteggendo dati sensibili e riservati sia da attacchi provenienti da utenti esterni, sia da usi non corretti attuati da utenti interni privilegiati.

]HackingTeam[

Mobile Device Management

MDM software protegge, controlla, gestisce e supporta i dispositivi mobili distribuiti attraverso operatori di telefonia mobile, service provider e aziende. Le funzionalità principale di MDM e' il controllo over-the-air (OTA) di applicazioni, dati e impostazioni di configurazione per tutti i tipi di dispositivi mobili, inclusi telefoni cellulari, smartphone, tablet PC.

Rilevamento anomalie

Anomaly detection

Meccanismi di controllo tecnologici volti alla rilevazione delle minacce di sicurezza e degli eventi anomali nel traffico di rete (monitoraggio attività di rete e sicurezza, IDS/IPS, NGFW).

Gestione dei log

Log management

Meccanismi di controllo tecnologici volti a regolare la genesi, la trasmissione, la memorizzazione e l'analisi dei log record (log collection, log retention, log correlation, log analysis, incident handling, monitoraggio asset tecnologici e applicativi, ...). Integrazioni con la soluzione DAM per il monitoraggio dei Database.

Attività investigative

Forensic analysis

Individuazione, acquisizione, conservazione, protezione, ricerca e documentazione di dati informatici per l'analisi di incidenti informatici. Le attività possono essere svolte sia per finalità interne all'organizzazione sia per finalità legali (evidenze processuali). Vengono impiegate procedure e metodologie standard volte a garantire la replicabilità di tutte le operazioni effettuate.

Nuove tecnologie

- Soluzioni di **Data Masking / Scrambling**
- Soluzioni ipad / iphone mobile file management: **Mobilecho**
- Soluzioni di *Network Knowledge*: **Netwitness**