]HackingTeam[

Profilo aziendale ed offerta

L’azienda in pillole

- Cosa: **sicurezza informatica (difensiva ed offensiva)**
- Come: **vendor independent**
- Quando: **fondata nel 2003**
- Chi: **i soci sono 3 persone fisiche e 2 fondi VC**
- Fatturato 2010: > **€ 4,2* mln.**
- Dipendenti: **35**
- Contatti: **http://www.hackingteam.it/contacts.html**

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
- Governo del rischio (Chi fa' cosa, quando e dove)
- Sicurezza Applicativa
- Rilevamento Anomalie
- Gestione dei Log
- Attività investigative

Alcuni clienti

ABI
ASSOCIAZIONE BANCARIA ITALIANA

BARCLAYS

ING DIRECT

Deutsche Bank

Agos DUCATO

CRIF

UBI Banca

ABN·AMRO

CASSA DI RISPARMIO
SPARKASSE

Cassa Centrale
CASSE RURALI TRENTINE - BCC NORD EST SpA

ACTALIS

Alcuni clienti

Alcuni clienti

Ethical Hacking

- Penetration test del perimetro interno ed esterno
- Simulazione profilo tipo (utente/consulente/fornitore)
- Web application hacking
- Wireless analysis
- Risk assessment mirati a componenti applicativi e Database
- ESX VMWARE
- VOIP
- 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

Controllo accessi

Controllo accessi

Insieme di politiche, processi, procedure e tecnologie volte ad aiutare un'organizzazione nella gestione degli accessi alle informazioni (identity & access management, SSO, autenticazione forte, autenticazione forte tokenless...).

DEEPNET SECURITY
SMART AUTHENTICATION

imprivata

CRYPTOCard

Virtualizzazione delle applicazioni

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.

Gestione delle password amministrative e dei privilegi utente

- Centralizzazione di politiche di controllo accessi per tutte le piattaforme e gestione degli account amministrativi di gruppo.
- Password vaulting e centralizzazione tramite AD dell'autenticazione e della gestione dei sistemi UNIX
- Estensione dei privilegi di base ai "normal user" su base nominale
- Integrazione "soft" con AD e configurazione basata su GPO
- Applicazione di politiche di "segregation of duties, audit logs e dinamic priviledge management
- Integrazione soft con i sistemi operativi Windows / Unix

beyondtrust
privilege. made simple

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.

Governo del rischio

- **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

Accesso remoto sicuro

- **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

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, protezione e audit DB, analisi applicativi proprietari, disponibilità dei servizi,...).

Rilevamento anomalie

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).

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, ...)

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**
- **Soluzioni di database audit e security: Sentrigo**
- **Soluzioni di Network Knowledge: Netwitness**
- **Soluzioni di WIFI sicuro: Aerohive**
- **Soluzioni di SSO “*client indipendent*”: Passwordbank**

Sicurezza offensiva....

RCS (Remote Control System)

- Soluzione di sicurezza offensiva sviluppata da HT
- Strumento utilizzato dalle LEAs (Law Enforcement Agency) per contrastare la criminalità organizzata e il terrorismo
- Permette di acquisire il controllo e di monitorare un target PC in modalità *stealth* e senza essere intercettato dalla maggior parte dei sistemi di protezione adottati per reti e computer
- Permette di intercettare ogni trasmissione generata o ricevuta dal target computer (es: mail, VOIP, files, Chat, P2P, ecc.)