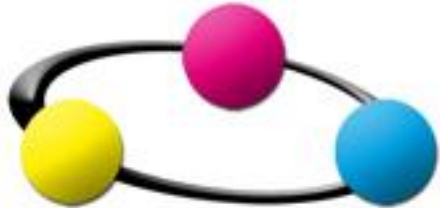


SECURITY



SUMMIT

Oracle Community For Security

Security Summit 2010

Corporate Forensics: dall'infrastruttura alla metodologia
Walter Furlan, CON.NEXO'

CON. NEXO'

Presentazione CON.NEXO'



CON.NEXO', in qualità di Partner ORACLE, è la prima azienda italiana in termini di fatturato, nell'erogazione dei servizi di outsourcing e supporto applicativo (Oracle Applications EBS, JDE, Oracle B.I.)

CON.NEXO' è un'azienda specializzata nella progettazione di sistemi organizzativi e gestionali e nell'erogazione di servizi innovativi che permettono il raggiungimento degli obiettivi di business dei clienti

CONSULTING & SERVICES Competence Center

- Oracle E-Business Suite
- Oracle J.D. Edwards
- Technologies and Security Consulting & Services
- SAP
- Business Intelligence and Data Warehouse
- Enterprise Project Management
- ICT Strategies & Governance



Il livello di informatizzazione delle realtà aziendali è in costante aumento

- Proliferazione di componenti elettroniche
- Necessità di essere collegati alla rete
- Utilizzo dei Social Network e Mail Box private dai sistemi aziendali
- WEB 2.0
- Cloud Computing

Resta invariato l'interesse per la tutela degli investimenti aziendali e dei diritti privati

- Avvalersi di diritti in sede legale
- Richiami disciplinari interni
- Permettere approfondimenti delle analisi
- Generare reportistica

La crisi economica genera mal contento e sfiducia. Quanto può fidarsi l'azienda dei dipendenti demotivati?

Conseguenze

Ne deriva l'esposizione a delle serie di rischi che devono essere quantomeno valutati

In ogni istante possono verificarsi eventi indesiderati ed assolutamente imprevedibili

- Attacchi informatici (interni ed esterni)
- Abusi dell'infrastruttura IT
- Violazione delle policy
- Furto di dati
- Attività di spionaggio

Questo comporta la necessità di controllo: se non possiamo prevenirli dobbiamo essere capaci di

- Identificarli
- Minimizzarne gli impatti

La disciplina della Computer Forensics, o più genericamente della Digital Forensics, applicata in un contesto aziendale può contribuire ad introdurre:

Metodologie

- Best Practices
- Procedure di validazione delle policy interne

Competenze

- Verticali, su come operare per acquisire, preservare ed analizzare i referti
- Orizzontali, su come identificare ed analizzare delle prove che coinvolgono svariate tecnologie

Infrastruttura (Log)

Le tecnologie di sicurezza probabilmente già adottate (Firewall, IDS/IPS, Proxy, IAM, DLP, Application Server, ecc..) generano LOG

Il log è solo un file di testo? Forse può avere altre caratteristiche...

Un log, trasmesso ed archiviato in modo opportuno può essere ritenuto:

- Integro
- Verificabile
- Immodificabile
- ...
- Storicizzato
- Ad alto valore

Questo richiede un'infrastruttura IT specializzata nella cui realizzazione vengano valutati con l'adeguato peso sia gli aspetti tecnologici sia gli aspetti giuridici.

Infrastruttura (Hardware)

Per avvalersi di una prova, è richiesto che la fonte sia *integra* e che l'operazione di estrapolazione della prova sia *ripetibile*. Questo comporta che la perdita di dati non è ammissibile

Hardware adeguato

- Storage opportunamente dimensionato
- Velocità bus
- Dimensioni Buffer
- Write Blocker

Infrastruttura (Tools)

Quali tools è meglio utilizzare?

- Cosa dobbiamo fare?
- Come va fatto?
- Qual è il risultato che ci aspettiamo di ottenere?

In base a cosa scegliamo un tool?

- Software Open Source
- Software Proprietari
- Sistema Operativo

Strumentazione (Performance)

In quanto tempo vogliamo gestire un incidente?

- Dimensioni medie di un disco rigido: 250GB
- Velocità media di lettura: 40MB/s
- Su un supporto comune, il tempo MINIMO di lettura del dato da analizzare: 2h
- Per OGNI operazione
- Dimensione media dei file: 400K
- Se non ci sono indizi che restringono il campo di analisi, vanno analizzati o quantomeno valutati circa 600.000 file
- ...
- Un supporto comune non è un supporto comodo da utilizzare per le analisi

Il laboratorio di analisi necessita di strumentazione performante

Strumentazione (Compatibilità)

Cosa dobbiamo analizzare?

- Log provenienti da fonti disomogenee (Firewall, IDS/IPS, Proxy, App Server, ecc..)
- PC/Mac/AIX/Solaris/HP-UX
- SmartPhone/SIM/PDA
- Stick-USB
- Compact Flash/SD
- Bus IDE/SATA/SCSI
- Backup Tape
- Ethernet/Fibra

Il laboratorio di analisi necessita di strumentazione che lo renda quanto più adattabile e compatibile alle sorgenti da analizzare

Metodologia (Best Practices)

La Corporate Forensics può essere un tema abilitante nella stesura di Best Practices interne che permettano di gestire gli incidenti:

Il referto deve essere:

- Identificato
- Acquisito
- Preservato
- Analizzato
- Tracciato
- Fruito esclusivamente da personale autorizzato

L'analisi dell'incidente deve essere:

- Gestita mediante un Work-Flow ben definito
- Documentata esaustivamente
- Riportata adeguatamente al Management

Metodologia (Validazione Policy)

La Corporate Forensics può inoltre fornire un approccio pragmatico e diversificato per verificare le policy e le misure di sicurezza adottate

Le policy e le misure di sicurezza devono essere:

- Esaustive
- Efficaci
- Adeguate
- Tutelanti
- Aggiornate periodicamente

La delicatezza dell'argomento richiede strutture e competenze specifiche che permettano di gestire le situazioni in modo adeguato

Struttura Forense

- Riconosciuta dagli utenti per facilitare le segnalazioni
- Autorizzata ad accedere ai sistemi da analizzare
- Supportata dal Management per renderla autorevole
- Abilitata ad accedere a competenze esterne

Team Forense

- Competente su Metodologie, Procedure e Legislazione di riferimento
- Formato ed Aggiornato sul piano tecnologico
- Disponibile ad intervenire prontamente

Le discipline forensi introducono metodologie e competenze, che possono essere sfruttate anche per finalità legittime ma non prettamente di tipo forense

Alcuni esempi:

- Verifica delle procedure di wiping dei dischi
- Verifica delle procedure di Data Recovery
- Simulazione furto di Notebook/SmartPhone/PDA
- Verifica dell'esposizione a Botnet/protocolli deboli/intercettazioni del traffico di rete
- Analisi Live e Software Reversing sui sistemi compromessi
- Troubleshooting su tecnologie di cui non sono noti i meccanismi di funzionamento
- Introduzione di Know-How nelle fasi di Design ed implementazione delle architetture IT

Grazie per l'attenzione

Per domande o commenti:

E-Mail: walter.furlan@connexo.it

Mobile: +39 393/9125678