Rete Dati di un polo Universitario: Strumenti e metodologie per la raccolta di prove in supporto alle indagini dell’Autorità Giudiziaria.

Implicazioni in ambito Privacy

(Università degli Studi di Milano, Facoltà di Giurisprudenza, 21 giugno 2012)

Il livello di Privacy cui noi aspiriamo è alto come la vetta di una montagna... ma sul percorso, nuvole s’adombrano...

Nicla Diomede  Donato La Muscatella  Marco Carlo Spada
Le Reti Universitarie
Ambiente Universitario

SERVIZI
- E-Mail
- Internet
- Servizi amministrativi
- Servizi per Studenti
- Aree condivise
- VoIP

UTENTI
- Studenti
- Professori
- Impiegati
- Ospiti

Nicla Diomede – Le Reti Universitarie
Caratteristiche della rete Universitaria

- Lo scenario considerato è di una rete complessa, estesa ed eterogenea:
  - Unica per Ricerca, Didattica, Amministrazione
  - Elevato (>70) numero di sedi distribuite sul territorio
  - Ambienti misti: presenza negli Ospedali
  - 65000 utenti
  - 40.000 punti cablati di cui circa 10.000 attivi
  - Cablata e wireless
  - Presenza promiscua nella stessa zona di varie tipologie di utenti appartenenti a strutture diverse

- Caratterizzato da:
  - Alta velocità
  - Affidabilità (ridondanza logica e fisica)
  - Supporto di servizi evoluti

- Interconnessa a Global Internet attraverso la Rete nazionale GARR
gli Enti fondatori (CNR, ENEA, INFN e la Fondazione CRUI);
• gli organismi di ricerca vigilati dal MIUR, tra cui ASI, INAF, INGV e altri;
• i Consorzi Interuniversitari per il Calcolo (CASPUR, CILEA, CINECA);
• Organismi culturali e di ricerca afferenti ad altri Ministeri, quali MiBAC e Salute;
• Rete ad altissima velocità collegata a:
  – rete della ricerca Europea
  – Global Internet
• Regolamentata da policy
I beni universitari

- L’università acquisisce, usa e memorizza informazioni relative ai suoi utenti: impiegati, docenti, pazienti, studenti, società con cui collabora.
- E’ necessario che questi dati siano gestiti in modo appropriato per prevenire la perdita, il danneggiamento, l’accesso o il furto delle informazioni.
- Il cattivo utilizzo, la perdita o compromissione comportano un costo economico, un danno d’immagine e possibili ripercussioni legali/penali.
- DATI UNIVERSITA’:
  - Proprietà intellettuale → ricerca, brevetti
  - Dati sensibili: dati medici
  - Dati amministrativi: dati del personale, stipendi, etc..
  - Dati legati al core business: dati carriera scolastica
  - Dati di studio per attività conto terzi
- La rete stessa è un bene
Criticità della sicurezza nelle Università

La sicurezza informatica è un problema

- complesso (coinvolge la rete, gli hosts e le persone),
- multilivello (tecnico, organizzativo, legale e sociale),
- in divenire (non è uno status, va costantemente mantenuta).

La sicurezza = protezione dei propri beni
≠ controllo o censura

L’Università NON è un azienda

Sicurezza  Facilità d’uso
LE POLICY UNIVERSITARIE (AUP)

- Forniscono un insieme di regole per la tutela della rete, degli host e dei servizi informatici.
- Sensibilizzare e responsabilizzare l’utenza: costituisce una sorta di carta dei diritti e dei doveri dell’utente dell’Università.
- Impedire che la rete universitaria possa essere fonte di attacchi verso l’esterno.

Immagine tratta da:
http://www.thetis.it/projects/transportation-management/urban-mobility-delhi.html
Acceptable Use Policy

- Tutti gli utenti devono essere riconosciuti ed identificabili;
- Uso per sole attività istituzionali
  
  E’ VIETATO

- fornire accesso a soggetti non autorizzati;
- Compiere attività (diffusione di virus, etc.) che danneggino, molestino o limitino le attività altrui o i servizi;
- creare o trasmettere materiale che attenti alla dignità umana, se non per motivi di ricerca
- Danneggiare o cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti,
- Pubblicizzare attività proprie per fini di lucro
- Attività vietata da leggi dello Stato
- -----
Il regolamento di Sicurezza

DEFINISCE
– Chi può accedere alla rete
– Come e dove accedervi:
  • LAN cablate
  • HOTSPOT, Wireless LAN, Eduroam
  • Biblioteche
  • Via vpn
  • Aule informatiche
– Protocolli consentiti
– Attività ammesse e non
– Identificazione degli utenti
– Responsabilità personali dei contenuti diffusi
– Sanzioni per trasgressori
– Misure minime per server centrali, locali e postazioni utente
– Ruoli nella gestione della sicurezza

LA REALTA’ E’ MOLTO COMPLESSA

Immagini Tratta da “Minority Report”
Gestione tecnica dell’infrastruttura simile a quella del provider:

- Estensione e complessità della rete
- Presenza promiscua e contemporanea di diversi tipologie di utenti appartenenti a strutture diverse
- Controllo e gestione totale dell’infrastruttura di rete
- Nessun controllo dei singoli pc/server locali gestiti in autonomia dalle singole strutture
- No controllo sull’accesso fisico alle sedi universitarie

Dal punto di vista giuridico il modello è quello privato:

- Rete riservata ai soli aventi diritto

Difficoltà di adottare policy stringenti di sicurezza:

- Eterogeneità utenti, vastità e molteplicità di utilizzo, libertà di ricerca
- Facilità di uso (autenticazione centralizzata per accesso alla rete solo in zone ad accesso pubblico)
Incidenti Informatici: > 500 all’anno
- Rete molto veloce, soggetta a continui tentativi di intrusione
- 10.000 host in rete
- Macchine con alte performance ma non sempre ben gestite di cui alcuni con risvolti penali/legali (richiesta A.G.)

RICERCA DEL COMPROMESSO TRA:
- Necessità di proteggere beni universitari
- Garantire livelli di servizio
- Tutelare l’ente da responsabilità (D. Lgs 231/2001)
- Tutelare la privacy degli utenti
- Garantire la conformità allo Statuto dei lavoratori
I Profili Giuridici
L’amministrazione delle Reti di questa complessità presenta, per lo studioso di ICT law, plurimi aspetti di interesse.
Cos’è l’ente amministratore della Rete?
Si tratta, sulla base di:

- copertura territoriale della rete;
- finalità di concessione dell’utilizzo della rete;
- logica dell’infrastruttura di rete interna;
- identificazione dei terminali utilizzati sulla Rete web.
di un soggetto (nel caso dell’Università degli Studi di Milano un’Amministrazione Pubblica) che offre e gestisce (in ispecie gratuitamente) una rete privata di comunicazioni elettroniche con funzioni istituzionali, sulla quale operano utenti identificati di diversa natura.
Nel caso preso ad esempio, infatti, la Rete dell’Università degli Studi di Milano, è collegata alla rete GARR, della quale accetta (e fa accettare all’utente) le policies.

... tuttavia...
Non sono utilizzati applicativi di controllo dell’attività degli utenti che impediscono la consultazione di siti web “non edu” (per garantire la ricerca ad ampio raggio).

... ergo ...
La Rete può essere utilizzata, potenzialmente, per navigazioni private, con scopi estranei a quelli per i quali il servizio di comunicazione elettronica viene predisposto e concesso in utilizzo all’utenza (ed eventualmente illeciti).
A ciò s’aggiunga il rischio proveniente da attacchi esterni all’infrastruttura, a tutt’oggi molto frequenti.
Pur non trattandosi di un ente assimilabile agli ISPs, trovano applicazione alcune modalità di regolamentazione dell’infrastruttura telematica ad essi riferiti.

Il monitoraggio della Rete, tuttavia, avverrà essenzialmente come attività di prevenzione rispetto a lesioni dei “beni aziendali”.

Donato La Muscatella – I Profili Giuridici
Pur non trattandosi di un ente assimilabile agli ISPs, trovano applicazione alcune modalità di regolamentazione dell’infrastruttura telematica ad essi riferiti.

Il monitoraggio della Rete, tuttavia, avverrà essenzialmente come attività di prevenzione rispetto a lesioni dei “beni aziendali”.
RESPONSABILITÀ

CONTROLLO

REGOLAMENTAZIONE IBRIDA
Questo tipo di qualificazione, come si vedrà, non è priva di effetti, tanto e gli obblighi dell’Istituzione universitaria, devono essere modulati anche in ordine ai diritti vantati dalle diverse categorie di utenti.
Che tipo di dati transitano sulla Rete?
Si tratta di dati personali e, in alcuni casi, sensibili degli utenti.

Peraltrò, anche i dati tecnici relativi alla trasmissione delle informazioni rientrano, secondo un orientamento che si sta diffondendo a livello comunitario, nella categoria dei dati sensibili.
Tra questi l’Avvocato Generale Jaaskinen che così si è espresso in relazione al caso *Bonner Audio* discusso dinanzi alla Corte di Giustizia dell’Unione Europea.

(vd. conclusioni del 19.11.2011, CGUE C-451/10)
Che tipo di utenti utilizzano la Rete?
Utenti Generici (studenti)

Questa tipologia di utenti, è tutelata dalle norme generali in materia di protezione dei dati personali.
Utenti Generici (studenti)

- informativa sul trattamento dei dati
- cosa
- come
- chi
- per quanto tempo
- che assicuri un’adeguata “informazione e consapevolezza”
- non è necessario il consenso al trattamento
Utenti Qualificati (lavoratori)

Questa classe di utenti, si giova di un ampliamento di protezione legato alla disciplina giuslavoristica.

In particolare, l’attività del lavoratore non può essere monitorata in tempo reale per verificare l’operato, anche sulla Rete.
Utenti Qualificati (lavoratori)

Sul punto, la Corte di Cassazione ha ritenuto legittimo, anche in assenza di accordo o autorizzazione preventiva “il monitoraggio delle strutture informatiche aziendali che prescinde dalla pura e semplice sorveglianza sull’esecuzione della prestazione lavorativa, ma è diretto ad accertare ex post la perpetrazione di eventuali comportamenti illeciti”

Utenti Qualificati (lavoratori)

- informativa sul trattamento dei dati formulata in modo specifico;
- non è necessario il consenso al trattamento;
- disciplinare interno redatto in modo chiaro e senza formule generiche;
- rispetto dei divieti assoluti di utilizzo (es. keyloggers, analisi occulta dei laptops, etc.)

(Delibera n. 13 del 01.03.2007 del Garante per la Protezione dei Dati Personali)
Utenti Qualificati (lavoratori)

Peraltro i datori di lavoro, anche pubblici, hanno l’onere di adottare “tutte le misure tecnologiche volte a minimizzare l’uso di dati identificativi” (cc.dd. PETs)

... ma...come?
Come *monitorare* l’attività della Rete?
Con il termine si intende:
✓ analisi dei dati relativi alle operazioni di comunicazione elettronica in senso stretto;
✓ analisi delle attività di navigazione web;
✓ analisi della corrispondenza telematica degli utenti assegnatari di un indirizzo e-mail

... che ne è della Privacy?
Alla luce di quanto detto, peraltro, i protocolli operativi dovranno tener conto del massimo livello di tutela possibile in rapporto alla categoria di utenti alla quale spettino maggiori garanzie.
Il trattamento dei dati, dovrà avvenire, in primo luogo, conformemente ai *principi* di

- necessità
- pertinenza
- non eccedenza
L’eventuale analisi dei dati, dovrà avvenire solo ed esclusivamente a posteriori, da personale autorizzato e per fini legalmente autorizzati.

inoltre
I files di log dovranno essere:

- lici (in relazione alla disciplina in materia di dati personali e tutela dei lavoratori);
- conservati in forma aggregata ed in formato grezzo;
- conservati per un periodo massimo di dodici mesi;
- identificabili solo dopo disaggregazione e correlazione delle informazioni;
- sovrascritti automaticamente allo scadere del periodo di data retention

mentre
Più opinabili sono:

✓ adozione di misure tecniche e organizzative adeguate al rischio esistente;

✓ comunicazione al Garante ed agli interessati “senza indebiti ritardi” di eventuali violazioni di dati personali (salvo inintellegibilità dei dati);

✓ adozione ed aggiornamento dell’inventario delle violazioni di dati personali

(cfr. D.Lgs. n. 69 del 28 maggio 2012, in vigore la 01.06.2012)
Come collaborare alle indagini?
Due le ipotesi in campo:

I. richiesta proveniente dall’Autorità Giudiziaria (artt.247, I bis, 253, 254 bis c.p.p.)

II. richiesta proveniente dal difensore (art. 391 quater c.p.p.)
In entrambi i casi bisognerà operare sul sistema se il soggetto presenti idoneo provvedimento o documentazione (decreto A.G. o atti di polizia giudiziaria relativi ai mezzi di ricerca della prova in ipotesi d’urgenza; richiesta di documentazione motivata del difensore).
consegnando i soli dati rilevanti in copia conforme all’originale, in forma aggregata ed in formato grezzo, riferiti al periodo oggetto di investigazione;

mantenendo integro e disponibile l’originale delle informazioni digitali consegnate sul sistema di amministrazione, evitandone la sovrascrittura;

sollecitando accertamenti tecnici urgenti, compiuti dalle Autorità competenti con ogni garanzia necessaria, qualora il sistema presenti rischi di instabilità.
ESEMPIO DI INFRASTRUTTURA
Infrastruttura di monitoraggio e raccolta di Dati relativi alla sicurezza provenienti da diverse fonti

Ha lo scopo di:

- individuare tempestivamente gli incidenti informatici attraverso sofisticate metodologie di detection e blocco automatico per alcuni di essi (limitare l’impatto all’esterno)
- Eventuali indagini interne
- Fornire le opportune risposte in caso di richiesta dell’AG

Correla, normalizza e priorizza le informazioni provenienti da più punti di osservazione al fine di ricostruire la dinamica dell’incidente/illecito

- Eventi di sicurezza IDS distribuiti in rete (analizzano tutto il traffico su rete geografica)
- Log server (DHCP, DNS, ..), log dei firewall e router,
- Analisi comportamentale degli host attraverso l’analisi traffico
  - Traffico backbone rete e server farm (Netflow v. 5)
  - Traffico IN/OUT verso la rete esterna GARR (netflow v.9)
SCHEMA ESEMPLIFICATIVO DELL’ARCHITETTURA
INFRASTRUTTURA DI RACCOLTA DEI DATI

Raccoglie, correla, conserva info di sicurezza consentendo la ricostruzione della dinamica dell’incidente

Nicla Diomede – Esempio di Infrastruttura
### Esempio di notifica di incidente:

<table>
<thead>
<tr>
<th>Offense 389</th>
<th>Offense Type</th>
<th>Source IP</th>
<th>Event Flow count</th>
<th>Start</th>
<th>Duration</th>
<th>Assignd to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnitude</td>
<td>Relevance</td>
<td>Severity</td>
<td>Credibility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Event Flow count</td>
<td>Event Flow count</td>
<td>439 Events and 5073 Flows in 4 categories</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP(x)</td>
<td>107.141</td>
<td>Local (2132)</td>
<td>36m 49s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination IP(x)</td>
<td>Multiple (102)</td>
<td>Not assigned</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network(s)</td>
<td>107.141, 231.140</td>
<td>Mexico</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>root</td>
<td>Vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>customer-107.141-231-140 stata.uninet-id México.com.mx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Name</td>
<td>Unknown</td>
<td>Asset Weight</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offenses</td>
<td>2</td>
<td>Events/Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Offense Source Summary**

<table>
<thead>
<tr>
<th>IP</th>
<th>Location</th>
<th>MAC</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>107.141, 231.140</td>
<td>Mexico</td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unknown</td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer-107.141-231-140 stata.uninet-id México.com.mx</td>
<td>Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events/Flows</td>
<td>5520</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Top 5 Source IPs**

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Magnitude</th>
<th>Location</th>
<th>Vulnerability</th>
<th>User</th>
<th>MAC</th>
<th>Weight</th>
<th>Offenses</th>
<th>Destination(s)</th>
<th>Last Event/Flow</th>
<th>Events/Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>107.141</td>
<td>102</td>
<td>Mexico</td>
<td>Unknown</td>
<td>root</td>
<td>unknown</td>
<td>0</td>
<td>2</td>
<td>2132</td>
<td>23 36m 19s</td>
<td>5520</td>
</tr>
</tbody>
</table>

**Top 5 Destination IPs**

<table>
<thead>
<tr>
<th>Destination IP</th>
<th>Magnitude</th>
<th>Location</th>
<th>Vulnerability</th>
<th>Chained</th>
<th>User</th>
<th>MAC</th>
<th>Weight</th>
<th>Offenses</th>
<th>Source(s)</th>
<th>Last Event/Flow</th>
<th>Events/Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>9</td>
<td>31</td>
<td>Unknown</td>
<td>No</td>
<td>Unknown</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td>1h 53m 11s</td>
<td>15</td>
<td>88</td>
</tr>
<tr>
<td>Unknown</td>
<td>15</td>
<td>25s</td>
<td>Unknown</td>
<td>No</td>
<td>Unknown</td>
<td>0</td>
<td>9</td>
<td>31</td>
<td>15m 25s</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>8</td>
<td>8</td>
<td>Unknown</td>
<td>No</td>
<td>Unknown</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td>2h 28m 53s</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>7</td>
<td>52s</td>
<td>Unknown</td>
<td>No</td>
<td>Unknown</td>
<td>0</td>
<td>11</td>
<td>29</td>
<td>1h 54m 21s</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>3</td>
<td>84</td>
<td>Unknown</td>
<td>No</td>
<td>Unknown</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>45m 57s</td>
<td>91</td>
<td></td>
</tr>
</tbody>
</table>

**Last 5 Notes**

<table>
<thead>
<tr>
<th>Notes</th>
<th>User Name</th>
<th>Create Date</th>
</tr>
</thead>
</table>

No results were returned.
### Segnalazione Incidente 2/2

#### Top 5 Log Sources

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Group</th>
<th>Events/Flows</th>
<th>Offenses</th>
<th>Total Events/Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS @ 159</td>
<td>IOS device</td>
<td>332</td>
<td>5</td>
<td>3681</td>
<td></td>
</tr>
<tr>
<td>IOS @ 159</td>
<td>IOS device</td>
<td>99</td>
<td>5</td>
<td>3254</td>
<td></td>
</tr>
<tr>
<td>Custom Rule Engine-8 : disco-unimi</td>
<td>Custom Rule Engine</td>
<td>8</td>
<td>524</td>
<td>5409</td>
<td></td>
</tr>
</tbody>
</table>

#### Top 5 Users

<table>
<thead>
<tr>
<th>Name</th>
<th>Events/Flows</th>
<th>Offenses</th>
<th>Total Events/Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>316</td>
<td>8</td>
<td>5800</td>
</tr>
<tr>
<td>bin</td>
<td>7</td>
<td>3</td>
<td>205</td>
</tr>
<tr>
<td>www</td>
<td>6</td>
<td>2</td>
<td>55</td>
</tr>
<tr>
<td>oracle</td>
<td>6</td>
<td>2</td>
<td>105</td>
</tr>
<tr>
<td>mircle</td>
<td>4</td>
<td>2</td>
<td>53</td>
</tr>
</tbody>
</table>

#### Top 5 Categories

<table>
<thead>
<tr>
<th>Name</th>
<th>Magnitude</th>
<th>Local Destination Count</th>
<th>Events/Flows</th>
<th>First Event/Flow</th>
<th>Last Event/Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misc Login Failed</td>
<td></td>
<td>2</td>
<td>4</td>
<td>03-13 15:14:45</td>
<td>03-13 15:47:52</td>
</tr>
<tr>
<td>User Login Failure</td>
<td></td>
<td>2</td>
<td>4</td>
<td>03-13 15:14:43</td>
<td>03-13 15:37:19</td>
</tr>
<tr>
<td>SSH Login Failed</td>
<td></td>
<td>2</td>
<td>431</td>
<td>03-13 15:14:33</td>
<td>03-13 15:49:52</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td>2</td>
<td>2132</td>
<td>03-13 15:11:45</td>
<td>03-13 15:40:17</td>
</tr>
</tbody>
</table>

#### Top 10 Events

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Magnitude</th>
<th>Log Source</th>
<th>Category</th>
<th>Destination</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Total Bytes</th>
<th>Last Packet Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:45:27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:48:13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:38</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:52</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:57</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:57</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:57</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%SSH-5-SSH2_USERAUTHFailed</td>
<td></td>
<td>IOS @ 159</td>
<td>SSH Login Failed</td>
<td>159</td>
<td>0</td>
<td>03-13 15:49:57</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Top 10 Flows

<table>
<thead>
<tr>
<th>Application</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Total Bytes</th>
<th>Last Packet Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteAccess:SSH_TCP_Allot</td>
<td>187 141</td>
<td>40281</td>
<td>159</td>
<td>22</td>
<td>2</td>
<td>2012-03-13 15:40:45</td>
</tr>
<tr>
<td>RemoteAccess:SSH_TCP_Allot</td>
<td>187 141</td>
<td>39847</td>
<td>159</td>
<td>22</td>
<td>2</td>
<td>2012-03-13 15:40:17</td>
</tr>
<tr>
<td>RemoteAccess:SSH_TCP_Allot</td>
<td>187 141</td>
<td>36115</td>
<td>159</td>
<td>22</td>
<td>2</td>
<td>2012-03-13 15:40:17</td>
</tr>
</tbody>
</table>
Dettaglio Flusso

Esempio dettaglio flusso sospetto connesso all’incidente con annesso l’elenco delle regole che si sono verificate e che hanno partecipato allo scatenarsi della segnalazione dell’incidente
Per gli eventi IDS è possibile consultarne i dettagli attraverso la console di visualizzazione del sistema IDS.
Premessa

La sicurezza implementata sull’infrastruttura di raccolta e conservazione dati è il compromesso tra

• complessità dello scenario,
• costi economici
• risorse umane

E

• probabilità di riuscita di un attacco verso una delle componenti della infrastruttura
• scopi della raccolta stessa.
Attività intraprese per PRESERVARE la fonte di prova e la protezione ai fini PRIVACY

I dati raccolti possano essere “prove” in ambito giudiziario se vi son garanzie di

• Disponibilità
• Autenticità
• Integrità

La messa in sicurezza di tutte le componenti dell’infrastruttura di raccolta e conservazione dei dati contribuiscono a dare le opportune garanzie in termini di normativa privacy.
Disponibilità dei dati

Server, firewall e router -> log a syslog server (syslog-ng ) soggetto a backup
LOG disponibili su:
- syslog server per un anno (conservato in modo compresso) e ruotati giornalmente
- server in locale (>= 1 mese)
- SIEM

Uso timestamping e firma digitale sui log archiviati a garanzia integrità e autenticità.
Eventi IDS:
- DB locale eventi ultimi 6 mesi;
- backup giornaliero su appliance dedicata: DB dell’ultimo anno in formato compresso e con garanzia di integrità
- SIEM
  - Meccanismi di hash su DB eventi e DB flussi
  - Retention personalizzabile su eventi, flussi e offese
- Infrastruttura di rete ridondata
Integrità e autenticità

In che modo garantirle?

Rendendo sicuri i dati memorizzati in fase di

- Generazione
  - Messa in sicurezza di ciascuna componente infrastruttura (server, router, IDS, firewall, SIEM)

- Trasmissione
  - Infrastruttura totalmente gestita anche a livello trasmissivo internamente,
  - controlli di integrità e crittografia dati, sistemi antintrusione e auditing

- Conservazione

- Controllo di accesso
  - Uso crittografia in comunicazioni tra IDS-SIEM e IDS-gestore IDS
Misure di sicurezza minime comune intraprese

Ciascun server erogante servizi di rete (DNS, DHCP, Auth,...) o appliance:
- Ridondato (solo server)
- Sincronizzato a NTP di Ateneo
- Posizionati in Server Farm ad accesso controllato
- Soggetto a Backup
- Configurata in DMZ dedicata (netmask /29 o /30)
- Installato e configurato seguendo le linee guida della NSA USA (server)
- Adozione di controlli di integrità sui file, di meccanismi antiintrusione e auditing
- Controllo accessi (compliance normativa AdS)
- S.O. linux o appliance con S.O. proprietario (derivato da linux)

Infrastruttura di rete a livello fisico, trasmissivo, logico gestita in modo autonomo (improbabile attacchi MiD)

Comunicazione crittografata:
- Sonde IDS -> gestore IDS;
- Gestore IDS → SIEM

Nicla Diomede – Esempio di Infrastruttura
Integrità e autenticità: su IDS

- IDS e gestore IDS su sottorete dedicata (netmask /30)
- IDS e gestore IDS connessi fisicamente ai router di backbone posti in locali protetti
- Password per il DB eventi
- S. O. proprietario
- ACL sui router coinvolti (accesso solo da sottoreti autorizzate) + iptables
- Host IDS sul gestore IDS (ad es. controlli integrità file)
- Sincronizzazione con il server NTP dell’Università (orario ufficiale).
- Comunicazione crittata:
  - IDS e gestore IDS
  - gestore IDS e suo backup
  - gestore IDS - SIEM (snmpv3 in modalità crittata).
- Accesso al gestore IDS tramite:
  - connessioni ssh2 da IP e utenti autorizzati.
  - applicativo proprietario basato su crittografia e autenticazione.
  - Visualizzazione DB degli eventi via SSL.

Nicla Diomede – Esempio di Infrastruttura
Integrità e autenticità: SIEM

- Configurazione su una sottorete dedicata (netmask /30)
- SIEM connessa fisicamente a router di backbone in locale protetto
- password per la scrittura nei DB
- S.O. proprietario hardened
- ACL sui router coinvolti (accesso solo da sottorete autorizzata) + iptables
- sincronizzazione NTP ateneo.
- Logging
- Comunicazione crittata:
  - Gestore IDS – SIEM
  - Accesso alla SIEM via ssh2 (ai soli ip e sistemisti responsabili del servizio);
  - Accesso alla console di SIEM via SSL.
- Hashing per i DB eventi e DB flussi
Integrità e autenticità: SERVER

- Configurazione su una sottorete dedicata (netmask /30-29)
- Server in DMZ d’Ateneo e fisicamente in Server Farm protetta
- Configurato secondo le linee guida della NSA-USA (National Security Agency)
- Iptables e ACL router
- Logging e invio al syslog server
- Hardening S.O.(attivazione anche SELinux)
- Disattivazione Mount dinamico/ supporto USB
- Permessi RWX personalizzati su file/directory.
- Update automatico del SW
- Attivazione di sistemi anti intrusione, SW di controllo di integrità, audit, antiDOS
- Accesso:
  - Via SSH solo da apposita sottorete e sistemisti autorizzati.
  - Disabilitazione root
  - modalità privilegiata via 2° livello autenticazione
  - Controllo accessi al sistema e ai suoi file/directory (partizioni per ogni user).
  - Protezione dell’accesso fisico alla console
- Crittografia dei filesystem
Integrità e autenticità: router

• Infrastruttura gestita, anche a livello trasmissivo, e manutenuta in totale autonomia
• Router in locali tecnici chiusi di proprietà universitaria
• Accesso solo da IP/tecnici autorizzati:
  • 1° Livello (RO): protocollo SSH2 con autenticazione via server AAA
  • 2° Livello (RW): tramite password locale dedicata
• Sincronizzazione NTP centralizzata
• Logging accessi
• Accesso fisico via console autenticato con server AAA
• ACL servizi locali (SSH, snmp, time etc.)
• ACL IN/OUT antispoofing
• ACL ulteriori sul router di bordo
CONCLUSIONI:

La piattaforma in oggetto può fornire utile supporto probatorio grazie a:

- adozione di opportune misure di sicurezza su ciascuna componente
- Rete totalmente gestita e mantenuta dall’Università
- bassa probabilità di buona riuscita di un attacco volto a eludere le misure
- Alto livello di competenza tecnica (expertise) richiesto
NETWORK FORENSICS
✓ che atteggiamento tengo come CTP a fronte del materiale informatico acquisito presso una rete di questo tipo?

✓ la terzietà del gestore della rete mi garantisce sempre e comunque?

✓ e un’analisi delle caratteristiche dei sistemi di raccolta e trasmissione delle tracce di rete ci può portare alla definizione di un insieme di “Best Practices” in tal senso?
✓ Cosa sono i Log?

✓ Quale è la loro principale funzione?

✓ Dove si trovano?
I Log: da dove vengono, come vengono trasferiti, come si presentano

**Apparati:**
- Switch
- Router/Firewall
- IDS
- Proxy Server
- Application Server

**Protocolli:**
- Syslog
- NetFlow

**Formati:**
- ASCII
- Binari
- pcap dump
- DB
È in linea teorica possibile:

- l’alterazione dei log attraverso la compromissione degli apparati
- l’alterazione dei log attraverso attività malevoli sulla rete
Lavori teorici sui log:

Bruce Schneier, John Kelsey - Secure Audit Logs to Support Computer Forensics - 1999

Steena Dominica Steven Monteiro, Robert F. Erbacher - An Authentication and Validation Mechanism for Analyzing Syslogs Forensically
Trasmissione dei log sulla rete:

- IEEE 802.
- IPv4
- UDP
- IPv6

VLAN – MAC ACLs
VPN – IPsec – Tunnelling – IP filtering
AH – ESP

Vantaggi con IPv6

(Bruce J. Nikkel - An introduction to investigating IPv6 networks - 2007)

- Migliore identificabilità degli apparati in forza dell’ampio spazio di indirizzi
- Scansioni più complesse per gli attaccanti
- AH ed ESP incorporati
Concludendo, un draft di proposta per best practices

- “Logs chaining and hashing”
- Adozione di modalità di trasmissione sicure e controllate
- Descrizione “a priori” del sistema di raccolta dei log
Q & A
Grazie per l'attenzione

Queste slide sono da utilizzare secondo i termini della Licenza Creative Commons: Attribuzione & Condividi allo stesso modo

Nicla Diomede  Donato La Muscatella  Marco Carlo Spada
Nicla Diomede  
nicla.diomede@unimi.it

Donato La Muscatella  
donato.lamuscatella@hotmail.it

Marco Carlo Spada  
m.c.spada@opimaint.it