Universita' di Padova
Progetto del GdL DREAMS
sicurezza informatica, wifi, firewall

Sicurezza informatica: aspetti tecnologici e normativi

Revisioni:

Versione	Data	Contributi	Status
1.0	Padova 18 dicembre 2007	GdL Sicurezza, AC	Prima redazione
1.1	Padova 17 gennaio 2008	GdL Sicurezza, AC	Bozza riveduta
1.2	Padova 18 gennaio 2008	Coord. DREAMS, AC	Correzioni, +formazione
1.3	Padova 5 febbraio 2008	AC	Stralcio

Breve descrizione del progetto:

Obiettivi: miglioramento della sicurezza informatica complessiva in Ateneo, attraverso (1) potenziamento della sicurezza perimetrale delle reti delle strutture periferiche (*firewall*), (2) regolamentazione delle reti *wireless* e (3) definizione di policy per la sicurezza coerenti e condivise.

Situazione esistente: in merito ai punti sopra evidenziati:

1 La rete di Ateneo e' topologicamente dispersa e molto frammentata: cio' comporta un considerevole dispendio di risorse nella sua gestione, con risultati assai eterogenei. E' importante fornire competenze e mezzi tecnici per raggiungere un livello uniforme di sicurezza e mutua fiducia tra le varie sottoreti di ateneo.

2 Sotto la pressione di una crescente domanda di reti wireless per didattica e ricerca, le varie strutture si stanno dotando autonomamente di punti di accesso wifi alla rete locale, con conseguenze potenzialmente molto serie sulla sicurezza. Inoltre soluzioni indipendenti e incompatibili portano a problemi di interoperabilita'. Vanno armonizzate e rese compatibili con le scelte di esternalizzazione delle reti wifi per gli studenti gia' operate in Ateneo.

3 La normativa nazionale (specie quella antiterrorismo) impone un contesto normativo molto severo che mal si adatta alle esigenze di una rete di ricerca e didattica. Questo spiega la ampia gamma di policy adottata dalle diverse strutture, pur nell'ambito delle stesse “linee guida per l'uso delle risorse informatiche di Ateneo”. Vanno definite delle esigenze minime in termini di accesso e gestione delle risorse, e aderenza alle esigenze della normativa nazionale (specie in merito alla tenuta delle registrazioni e all';identificazionedegli utenti).

Le conseguenze piu' critiche che ne conseguono e che il progetto intende affrontare sono: strutture periferiche sprovviste di firewall, access point wireless sprovvisti di misure efficaci di sicurezza, possibili furti di identita' e violazione della privacy, mancata ottemperanza alla normativa in merito alla tenuta di registrazioni.

Criticità: Le criticita' in merito al successo del progetto sono da mettere in relazione principalmente con la definizione di policy che potrebbero non essere accolte in quanto eccessivamente restrittive per i contesti in cui ne vigono altre piu' elastiche. Il successo

dell'iniziativa dipendera' anche dal successo delle attivita' di formazione.

Motivazione: La sicurezza informatica in Ateneo presenta ampie disomogenita' e potenziali difformita' rispetto alla normativa vigente e alle buone prassi. E' opportuno iniziare tempestivamente un processo che porti a una maggiore convergenza, partendo dall'esistente.

Attività previste: le attivita' mireranno a:

1. produrre delle **linee guida relative alle reti wireless** sviluppate internamente e raccomandazioni per quelle destinate agli studenti per le quali l'Ateneo ha provveduto con accordi di outsourcing.
2. produrre un **documento di presa in carico** che consenta ad utenti (specie di ricerca) che non sono inquadrati come tecnici informatici ma che che ne hanno le competenze di gestire con la necessaria autonomia risorse informatiche connesse alla rete di Ateneo.
3. Produrre documentazione in merito alle prassi di tenuta delle registrazioni previste per legge
4. produrre un **insieme di regole** per firewall che siano utilizzabili dalle varie strutture secondo la loro tipologia, usando le risorse esistenti
5. in relazione con il punto (d), realizzare un **servizio** web che renda agevole lo scambio delle informazioni necessarie per la manutenzione dei firewall delle varie strutture
6. in relazione con il punto (d), realizzare uno **studio di fattibilita'** in merito alla possibilita' di produrre, collaudare, distribuire e manutenere un **firewall** per ciascuna delle strutture che non dispongono di firewall e/o di tecnici informatici.
7. Attivita' trasversali alle precedenti di formazione e disseminazione.

Strutture coinvolte: quelle del personale partecipante:
Presidenze di facolta': Lettere e Giurisprudenza, Ingegneria
Dipartimenti: DEI, Diritto Comparato, Fisica, Scienze Economiche, Scienze Statistiche
Centri: CiS Madura, CCA

Competenze necessarie: Informatiche: networking, sicurezza informatica, reti wireless, cablaggi. Legali: privacy, tenuta di registrazioni (decreto Pisanu) e responsabilita' dell'Ateneo.

Risorse umane necessarie: fanno parte del gruppo di lavoro:

1. Alvise Belotti (Pres. F. Lettere)
2. Alberto Cammozzo (Dip. Sc. Statistiche)
3. Marco Filippi (DEI)
4. Francesco Gasparini (Dip. Dir. Comparato)
5. Gianluca Giacometti (Pineca – Presidenza di Ingegneria)
6. Michele Magon (Pres. F. Giurisprudenza)
7. Mauro Malvestio (Dip. Sc. Statistiche)
8. Davide Marangon (CIS Maldura)
9. Riccardo Marcon (Dip. Sc. Economiche)
10. Simone Marzola (CCA)
11. Matteo Menguzzato (Dipartimento di Fisica)
12. Giorgio Paolucci (CCA)
13. Steno Varaschin (CCA)

Destinatari: tutte le strutture di Ateneo

Costi stimati: Le attivita' prevedono riunioni e attivita' individuali. Le riunioni tra i partecipanti

dal gruppo di lavoro sono stimabili in un incontro mensile di circa 3/4h per 12 persone. La stima di circa 500 ore/persona e' piuttosto grossolana non tenendo conto delle assenze. Altrettanto va stimato per lo svolgimento delle attivita' individuali, che coinvolgeranno in modo variabile i singoli partecipanti. Il totale puo' essere approssimato in circa 800/1000 ore/persona.
Se dallo studio di fattibilita' emergesse la necessita' di procedere fino alla realizzazione di un firewall per le strutture non gestite servira' dell'hardware sul quale sviluppare il sistema, presumibilmente con un costo contenibile entro i 1000 Euro.

Rischi stimati: non presenti

Benefici previsti: l'aumento della sicurezza dovrebbe portare benefici immediati tangibili in termini di sicurezza reale (minor numero di eventi collegabili a insicurezza informatica) e percepita (maggior fiducia dell'utente nella sicurezza dei sistemi). In particolare ci si attende:

1. un abbattimento del rischio di procedimenti giudiziari e/o richieste di risarcimento
2. una riduzione delle richieste dell'autorita' giudiziaria e di attivita' di ripristino in seguito a guasti prodotti da scarsa sicurezza. Di conseguenza e' prevedibile una maggiore produttivita' del personale e minori costi
3. un abbattimento dei costi di transazione interni come conseguenza di una maggiore collaborazione e di una maggiore omogeneita' delle policy e delle regole relative alla sicurezza
4. ottenere una “mappatura” dei servizi informatici di Ateneo

Risultati attesi: In seguito all'adozione delle linee guida, ci si attende una maggiore uniformita' del livello complessivo di sicurezza. Nel corso dei lavori ci si attende di rendere conoscenza esplicita e gestita una serie di informazioni sui servizi interni. Uno dei risultati attesi e' anche, per effetto della formazione, quello di elevare il livello di consapevolezza sulle problematiche di sicurezza e sulla necessita' di policy aderenti sia alle esigenze degli utenti che alle normative.

Tempistica
La maggior parte dei documenti dovrebbero essere prodotti nel corso del 2008, alcuni con scadenze anche brevi (quello della commissione per i log, presa di responsabilita' per i dipendenti non tecnici informatici). Il progetto di firewall, piu' articolato, si estendera' prevedibilmente fino al 2009 con dei risultati intermedi scanditi in queste fasi:

1. Un ruleset di base consigliato per un firewall generico adatto alle varie tipologia di struttura riscontrabile in Ateneo
2. Un servizio che renda le informazioni del punto precedente accessibili e aggiornabili da chi fornisce i servizi frubili da tutto l'Ateneo (ad esempio mail server) in modo che siano attendibili e autorevoli.
3. Un firewall (l'apparecchio fisico) da dare alle strutture che non dispongono di competenze e personale. Questo passo richiedera' (se stimato realizzabile) tempi lunghi perche' comporta la valutazione sulla creazione di un vero e proprio servizio.

Prodotto finale: come descritto nella sezione Attivita'. Si produrranno documenti e linee guida, regole per firewall (formalismi per calcolatore) ed eventualmente sistemi informatici completi (firewall).

Estensore del rapporto: A.Cammozzo