ITAS Assicurazioni

Studio della sicurezza interna e delle agenzie

Sintesi dei risultati e proposta di risoluzione dei problemi riscontrati

Trento

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

Premessa

L'obiettivo del presente documento consiste nel fornire un quadro sintetico dello stato della sicurezza interna e di agenzia di ITAS Assicurazioni.

La terminologia utilizzata è volutamente di alto livello e questo conferisce al documento un carattere decisamente non tecnologico. Quello che si vuole evidenziare sono esclusivamente i problemi, la loro criticità e la loro possibile risoluzione.

Il documento è suddiviso in tre parti:

1) PARTE I: sintesi del lavoro svolto e descrizione delle problematiche di sicurezza riscontrate
2) PARTE II: classificazione delle minacce e identificazione delle macro-aree di intervento
3) PARTE III: proposta di piano esecutivo per la copertura delle minacce di sicurezza e per la sistemazione delle problematiche rilevate

Nella proposta di risoluzione/intervento di ogni macro-area verranno elencate (ove presenti) più soluzioni e, per ognuna di esse, verrà indicato lo sforzo interno richiesto. Questo sta ad indicare la proposta è stata studiata seguendo due linee guida principali:

1) Criterio di minima: ove possibile si tende ad utilizzare
    a. strumenti già esistenti nell'infrastruttura tecnologica di ITAS
    b. risorse interne del cliente
2) Criterio di supporto: ove possibile si tende ad utilizzare l'esperienza e le competenze di Hacking Team a supporto dell'esecuzione.

Si ritiene importante sottolineare che in parallelo alle attività proposte è necessaria un'analisi della profilatura attuale degli utenti, basata su criteri di utilizzo delle risorse e delle applicazioni. In altre parole è indispensabile sapere "chi fa cosa" e "chi è autorizzato a fare cosa" nel vostro sistema informativo.

Parte I – Sintesi dei risultati

Il presente documento descrive le attività svolte da HackingTeam S.r.l. relativamente al progetto di revisione della sicurezza della rete interna di ITAS Assicurazioni.
L'approccio alle attività segue una linea comune: ognuna di esse ha come obiettivo quello di mettere in evidenza possibili debolezze dei sistemi, sfruttabili da una persona *malintenzionata* con intenti fraudolenti o dannosi per il business del cliente.
Le metodologie e le tecniche utilizzate dal personale HackingTeam sono del tutto paragonabili a quelle utilizzate da veri *"hacker"*: ripercorrendo il percorso logico di un attacco reale é stato possibile accertare i punti deboli dell'infrastruttura informatica del cliente e, qui di seguito, fornire le soluzioni ai problemi riscontrati.

I risultati dell'attività di analisi della sicurezza si rivelano particolarmente interessanti poiché mettono in evidenza alcune gravi lacune che rendono la rete interna di ITAS Assicurazioni vulnerabile anche ad attacchi che non richiedono necessariamente delle conoscenze informatiche elevate. L'attività di *analisi della sicurezza* svolta **dall'interno** della rete del cliente, ha permesso di **entrare in possesso di dati assolutamente sensibili e riservati** come le informazioni relativi alla gestione del personale (ad esempio tabelle degli stipendi), i dati degli assicurati, le informazioni di natura finanziaria (ad esempio numeri di conto corrente bancari), ecc. L'analisi mette in evidenza la fragilità dei sistemi interni contro attacchi portati da postazioni di lavoro attestate sulla normale rete, utilizzata dagli utenti di sede.
Le tecniche utilizzate per attaccare e compromettere i sistemi strategici sono da considerarsi accessibili anche da persone con un basso "profilo tecnico"; praticabili quindi anche da individui non prettamente provenienti da un background di sicurezza informatica. In sintesi anche un utente non particolarmente "formato" tecnicamente potrebbe accedere a dati riservati utilizzando strumenti facilmente reperibili sul web. Gli impatti sul business aziendale sono di notevole importanza e non sono sicuramente da trascurare. Nel giro di poche ore, i consulenti di HackingTeam Srl. sono riusciti ad ottenere un accesso ai sistemi strategici della rete di ITAS Assicurazioni quali:

- Tutti i server e le workstation di Dominio ITASNET:
  - Server di Posta,
  - file servers,
  - sistemi applicativi (su tutti SAP)
  - personal computer degli utenti
- Apparati di instradamento (switch)
- Centralino telefonico
- Storage server
- Database server

L'accesso non autorizzato a questi sistemi mette in condizione un eventuale malintenzionato di avere a disposizione l'intero sistema informativo di ITAS Assicurazioni, consentendogli di accedere a documenti riservati, dati personali e sensibili protetti dalla legislatura, ecc.
La cattura di queste informazioni e l'eventuale diffusione possono avere implicazioni legate:

- al business del cliente,
- di natura legale,
- all'immagine ed alla credibilità del cliente

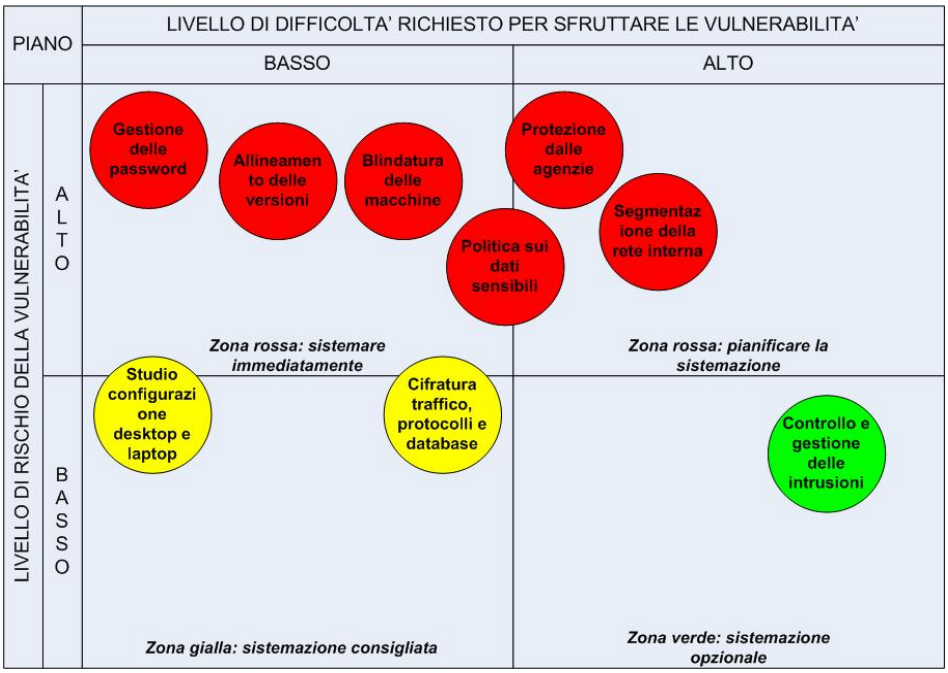
di conseguenza questi risultati sono da tenere in massima considerazione.

Un altro scenario importante é quello che si presenta arrivando dalla **rete di agenzia**: il personale di agenzia ha la possibilità di accedere a tutti i servizi offerti dal sistema informativo di ITAS Assicurazioni, anche a quelli non strettamente necessari (ad esempio i servizi di amministrazione remota, documenti prettamente interni ed altre risorse condivise).
É superfluo ribadire il concetto che ogni servizio lascito aperto può divenire una porta di accesso al sistema se la sua sicurezza non è opportunamente curata.
Ciò lascia la possibilità ad un potenziale malintenzionato che agisce da una agenzia, di ripetere gli scenari di attacco descritti in questo documento, anche da una postazione remota (cioè dalla rete di agenzia). L'intrusione in questi sistemi non solo ha un impatto diretto sui sistemi in questione, ma può avere ripercussioni maggiori: infatti sfruttando i sistemi di sede attaccati, é possibile agire contro altre agenzie (lettura, modifica e cancellazione del portafoglio) o addirittura portare un attacco alla rete interna di ITAS Assicurazioni.
Con le informazioni in possesso, é plausibile ritenere che tali eventualità sono tutt'altro che remote; di conseguenza, é fortemente consigliato intraprendere il più presto possibile le azioni correttive esposte nel documento, per scongiurare possibili danni al business legati a queste delicate problematiche.

Concludendo, l'attività di Analisi della sicurezza di HackingTeam **ha evidenziato condizioni di alta criticità** nella sicurezza dei sistemi di ITAS Assicurazioni; vista la natura delle informazioni trattate e dell'importanza dei sistemi in gioco, la messa in atto delle contromisure consigliate risulta di vitale importanza per scongiurare i rischi messi in evidenza dall'attività di progetto.
Nel presente documento sono descritte, in sintesi, le attività effettuate, le problematiche riscontrate e, per quanto è stato possibile, i rimedi atti a prevenire e/o arginare le conseguenze di una violazione dei sistemi suddetti.
HackingTeam, avendo già affrontato situazioni analoghe presso numerosi clienti soprattutto in ambito assicurativo e bancario, è qualificata a collaborare con ITAS Assicurazioni per fornire tutta la consulenza, tecnologica ed organizzativa, necessaria affinché le suddette attività siano svolte nel miglio modo possibile; l'adozione delle soluzioni proposte deve, a nostro avviso, andare di pari passo con una rivisitazione organizzativa degli accessi alle risorse del sistema informativo.

Parte II – Piano di copertura delle vulnerabilità

Le vulnerabilità di sicurezza rilevate durante l'analisi sono state raggruppate in macro-aree per meglio identificare la tematica alla quale si riferiscono. Nel grafico seguente, tali macro-aree vengono posizionate in base alla loro gravità e quindi in base alla loro urgenza e priorità di sistemazione.
Il grafico descrive nelle ascisse il livello di competenze che deve avere un malintenzionato per poter portare a compimento le proprie azioni; nelle ordinate il livello di rischio a cui è sottoposto il sistema informativo del cliente.



Questa rappresentazione porta il grafico a catalogare le macro-aree di intervento in quattro classi:

1. Macro-aree su cui intervenire il prima possibile (area rossa in alto a sinistra)
    a. Competenze da avere: BASSE
    b. Livello di rischio: ALTO
2. Macro-aree su cui intervenire in maniera pianificata (area rossa in alto a destra)
    a. Competenze da avere: ALTE
    b. Livello di rischio: ALTO
3. Macro-aree su cui si consiglia di intervenire (area gialla)
    a. Competenze da avere: BASSE
    b. Livello di rischio: BASSO

4. Macro-aree su cui non è urgente intervenire (area verde)
    a. Competenze da avere: BASSE
    b. Livello di rischio: BASSO

Di seguito, si descrivono sinteticamente le macro-aree.

GESTIONE DELLE PASSWORD

Essendo già presente una politica di impostazione, utilizzo e cambio delle password, occorre implementare un sistema di controllo che ne verifichi l'applicazione. E' inoltre indispensabile semplificare il lavoro degli utenti aiutandoli nella gestione delle loro password e sensibilizzandoli sull'argomento. Tutto ciò si traduce da una parte in un sensibile aumento del livello di sicurezza, dall'altra in una riduzione dei costi/tempi di gestione da parte degli amministratori IT.

ALLINEAMENTO DELLE VERSIONI ED APPLICAZIONE DELLE PATCH DI SICUREZZA

I sistemi informativi devono essere allineati all'ultima versione e protetti mediante installazioni delle patch di sicurezza. Questo ovviamente previa verifica in un ambiente di test adeguato. Qualora alcune attività non si potessero fare, è consigliabile avere delle politiche e delle procedure di gestione che prevedano un controllo ad hoc più stringente.

BLINDATURA E CONFIGURAZIONE AVANZATA DELLE MACCHINE

Seguendo le best practices esistenti in materia di sicurezza informatica, si deve procedere alla messa in sicurezza (blindatura) delle macchine per prevenire: accessi abusivi alle risorse aziendali, manipolazioni dei dati da parte di personale non autorizzato.

POLITICA DI UTILIZZO DEI DOCUMENTI E DEI DATI SENSIBILI

Occorre definire una politica solitamente chiamata "clean desk" che definisca le regole di utilizzo del materiale e dei dati sensibili (in termini di privacy), confidenziali (in termini di business) e critici (in termini di sicurezza); siano essi cartacei (scrivania, stampante o parti comuni) o digitali (postazione locale dell'utente).

PROTEZIONE DALLE AGENZIE

Occorre salvaguardare i sistemi centrali sia da internet che da personale extranet (non dipendente) garantendo il cliente che ogni persona possa raggiungere ed utilizzare le sole risorse delle quali necessita per compiere il proprio lavoro.

SEGMENTAZIONE DELLA RETE INTERNA

Un'adeguata strutturazione e suddivisione della rete interna permette di distinguere un utente da un amministratore, un server da un consulente, e così via. Questo tipo di architettura porta il sistema ad essere più gestibile, più controllabile e di conseguenza più sicuro.

STUDIO CORRETTA CONFIGURAZIONE DI DESKTOP E LAPTOP

E' importante definire la corretta e sicura configurazione da utilizzare nell'installazione dei desktop e dei laptop. Ad essa deve seguire necessariamente la definizione di procedure di controllo, di verifica e di aggiornamento del parco macchine.

CIFRATURA DEL TRAFFICO, DEI PROTOCOLLI E DEL DATABASE

Ove possibile, è consigliabile l'utilizzo della cifratura per rendere i dati confidenziabili e non facilmente accessibili. Si parla di cifratura del traffico (per motivi di confidenzialità dei dati) dei protocolli (per motivi di sicurezza) e del database (per motivi di privacy).

CONTROLLO E GESTIONE DELLE INTRUSIONI

Sarebbe utile definire una politica e le relative procedure per l'identificazione, il controllo e la gestione delle intrusioni o delle non-aderenze alle politiche aziendali. Si tratta di definire un sistema di gestione degli incidenti informatici.

Parte III – Proposta di lavoro

Di seguito verrà dettagliata la proposta di lavoro, suddividendola per ogni macro-area. Ove possibile (in base all'ambiente di riferimento, alla tipologia del cliente e del suo sistema informativo) si specificheranno più soluzioni al problema. Tutte le soluzioni indicate hanno l'ovvio beneficio di innalzare notevolmente il livello di sicurezza attuale.

Gestione password

Soluzione A: "Gestione manuale interna"	
Descrizione attività	1. Sistemazione manuale delle password deboli. 2. Controllo della politica e delle procedure esistenti, definizione ed applicazione di sistemi manuali di controllo e verifica. 3. Sensibilizzazione e comunicazione interna.
Benefici	• Aumento del livello di sicurezza • Sensibilizzazione degli utenti alla tematica
Punti di forza	• Applicabilità immediata • Nessuno strumento aggiuntivo • Maggiore autonomia realizzativa
Punti di debolezza	• Notevole sforzo di verifica e di modifica • Invariato il numero di password di ogni utente • Maggiore probabilità di errori • Non vi è garanzia del rispetto della politica definita • Maggiori costi interni di gestione ripetuti negli anni
Costi	**Interni**
	• Tempo uomo per la definizione delle procedure • Tempo uomo per la sistemazione delle password attuali • Tempo uomo per i controlli futuri • Tempo uomo per le attività di help-desk (password dimenticate e così via)
	Esterni
	• Affiancamento a supporto delle attività 1 e 2

Soluzione B: "Gestione automatizzata delle password"	
Descrizione attività	1. Definizione delle politiche di utilizzo delle password e del sistema 2. Progettazione e implementazione del nuovo sistema 3. Configurazione delle regole stabilite
Benefici	• Sensibile aumento del livello di sicurezza • Importante sensibilizzazione degli utenti alla tematica • Automatizzazione del ciclo di vita delle password • Maggiore aderenza ai requisiti stabiliti dalla legge sulla privacy
Punti di forza	• Notevole semplicità d'uso per utenti ed amministratori • Riduzione dei tempi di help-desk • Riduzione dei costi di gestione • Applicabilità immediata
Punti di debolezza	• Adozione di un nuovo strumento • Diminuzione delle attività di progetto eseguibili autonomamente

Costi	**Interni**
	• Tempo uomo per la definizione delle politiche • Tempo uomo per seguire le attività di progetto • Tempo uomo per l'apprendimento dell'uso del nuovo sistema
	Esterni
	• Acquisto e manutenzione dello strumento • Acquisto dell'hardware necessario • Consulenza per la realizzazione del progetto

Allineamento delle versioni ed applicazione delle patch di sicurezza

Soluzione: "Aggiornamento manuale"	
Descrizione attività	1. Analisi dello stato attuale delle macchine 2. Definizione del piano di testing per versioni e patch 3. Verifica ed aggiornamento delle macchine in produzione
Benefici	• Eliminazione delle vulnerabilità derivanti da sistemi non aggiornati
Punti di forza	• Sistemi allineati e privi di bachi software • Verifica puntuale con il minimo impatto sui sistemi
Punti di debolezza	• Attività esclusivamente manuale
Costi	**Interni**
	• Tempo uomo per l'analisi dell'esistente • Tempo uomo per la fase di testing e aggiornamento
	Esterni
	• Affiancamento a supporto delle attività

Blindatura e configurazione avanzata delle macchine

Soluzione: "Blindatura manuale"	
Descrizione attività	1. Analisi dello stato attuale della configurazione delle macchine 2. Verifiche dell'applicabilità delle modifiche 3. Impostazione sulle macchine di produzione
Benefici	• Diminuzione del rischio di incidenti informatici e di disservizi
Punti di forza	• Macchine maggiormente protette
Punti di debolezza	• Attività esclusivamente manuale
Costi	**Interni**
	• Tempo uomo per la definizione delle procedure di blindatura • Tempo uomo per seguire le attività
	Esterni
	• Consulenza per lo svolgimento delle attività

Politica di utilizzo dei documenti e dei dati sensibili

Soluzione: Definizione della politica	
Descrizione attività	1. Condivisione e definizione degli obiettivi 2. Definizione e stesura della politica di clean-desk 3. Definizione e stesura delle procedure di controllo
Benefici	• Sensibilizzazione degli utenti alla tematica • Minore dispersione dei dati sensibili/critici
Punti di forza	• Nessun impatto tecnologico • Costi contenuti
Punti di debolezza	• Forte impatto organizzativo e procedurale • Forte delega agli utenti
Costi	**Interni**
	• Tempo uomo per la definizione della politica e delle procedure • Tempo uomo per i controlli periodici
	Esterni
	• Affiancamento a supporto delle attività iniziali

Protezione dalle agenzie

Le soluzioni possibili sono molte e di vario tipo a seconda dell'obiettivo aziendale, del tipo di ambiente tecnologico esistente e della valutazione costi-benefici. Un elenco appropriato e coerente con la realtà del cliente potrà essere redatto solo dopo uno studio preliminare. E' per tale motivo che la sistemazione di questa macro-area è stata posizionata fra quelle da pianificare con attenzione.

Soluzione: Studio di fattibilità preliminare	
Descrizione attività	1. Analisi approfondita della situazione attuale 2. Definizione degli obiettivi ed identificazione della soluzione ottimale 3. Progettazione della soluzione e definizione di un macro-piano dei lavori
Benefici	• Approccio e risoluzione di un problema grave in modo strutturato e di ampio respiro • Conoscenza approfondita dei flussi informativi e dei processi esistenti fra centro e periferia
Punti di forza	• Maggiore accuratezza nell'analisi e nella definizione della soluzione • Maggiore coinvolgimento della struttura aziendale (interna ed esterna) • Maggiore durata della soluzione • Vendibilità e sensibilizzazione dei collaboratori esterni
Punti di debolezza	• Allungamento dei tempi di sistemazione della vulnerabilità
Costi	**Interni**
	• Tempo uomo per la raccolta iniziale delle informazioni
	Esterni
	• Consulenza per l'attività di studio fattibilità e progettazione

Segmentazione della rete interna

Le soluzioni possibili sono molte e di vario tipo a seconda dell'obiettivo aziendale, del tipo di ambiente tecnologico esistente e della valutazione costi-benefici. Un elenco appropriato e coerente con la realtà del cliente potrà essere redatto solo dopo uno studio preliminare. E' per tale motivo che la sistemazione di questa macro-area è stata posizionata fra quelle da pianificare con attenzione.

Soluzione: Studio di fattibilità preliminare	
Descrizione attività	1. Analisi approfondita della situazione attuale 2. Definizione degli obiettivi ed identificazione della soluzione ottimale 3. Progettazione della soluzione e definizione di un macro-piano dei lavori
Benefici	• Approccio e risoluzione di un problema grave in modo strutturato e di ampio respiro • Conoscenza approfondita dei flussi informativi e dei processi esistenti nella rete interna
Punti di forza	• Maggiore accuratezza nell'analisi e nella definizione della soluzione • Maggiore durata della soluzione • Maggiore capacità di controllo e gestione dei flussi informativi aziendali
Punti di debolezza	• Allungamento dei tempi di sistemazione della vulnerabilità
Costi	**Interni**
	• Tempo uomo per la raccolta iniziale delle informazioni
	Esterni
	• Consulenza per l'attività di studio fattibilità e progettazione

Studio corretta configurazione desktop e laptop

Nonostante la presenza ormai consolidata di nuovi strumenti per il controllo delle attività degli utenti e del rispetto delle politiche aziendali, riteniamo prematuro consigliarvi la loro adozione in questo momento di iniziale approccio alla sicurezza aziendale.

Soluzione: Rafforzamento della configurazione delle postazioni	
Descrizione attività	1. Analisi della configurazione attuale di desktop e laptop 2. Definizione di una politica di utilizzo del pc aziendale 3. Definizione delle variazioni di configurazione necessarie 4. Test di usabilità in produzione su un parco macchine limitato
Benefici	• Migliore e più sicuro utilizzo delle risorse aziendali • Uniformità dell'installato
Punti di forza	• Miglioramento della gestione del parco macchine • Riduzione della possibilità di incidenti informatici • Diminuzione del carico di lavoro dell'help-desk
Punti di debolezza	• Intervento su tutto il parco macchine installato • Minore libertà di azione sulla propria postazione da parte degli utenti
Costi	**Interni**

	• Tempo uomo per l'analisi e la definizione delle nuove impostazioni • Tempo uomo per l'applicazione di quanto definito
	Esterni
	• Affiancamento a supporto delle attività iniziali

Cifratura del traffico, dei protocolli e del database

Soluzione A: Analisi per l'utilizzo della cifratura	
Descrizione attività	1. Breve analisi di cosa cifrare in termini di traffico, protocolli e database 2. Scelta del meccanismo più opportuno e definizione di un piano dei lavori per la messa in sicurezza del traffico sensibile/critico 3. Scelta del meccanismo più opportuno e definizione di un piano dei lavori per la messa in sicurezza dei protocolli sensibili/critici 4. Scelta del meccanismo più opportuno e definizione di un piano dei lavori per la messa in sicurezza dei database ospitanti dati ritenuti sensibili/critici
Benefici	• Aumento della confidenzialità dei dati • Maggiore protezione dei dati sensibili
Punti di forza	• Diminuzione della possibilità di accesso non autorizzato a dati sensibili e critici • Aumento dell'aderenza alle normative sulla privacy
Punti di debolezza	• Utilizzo di nuovi strumenti e nuove tecnologie
Costi	**Interni**
	• Tempo uomo per seguire le attività di progetto • Tempo uomo per l'apprendimento dell'uso dei nuovi sistemi
	Esterni
	• Consulenza per l'attività di analisi iniziale e di progetto • Eventuale costo degli strumenti di cifratura[1]

Controllo e gestione delle intrusioni

Soluzione A: Gestione manuale degli eventi critici	
Descrizione attività	1. Definizione e stesura di una politica di avviso e allarmistica (alerting e alarming) adeguatamente corredata da procedure tecniche esecutive 2. Identificazione delle configurazioni necessarie al rilevamento 3. Definizione e stesura di una politica di gestione degli incidenti (incident handling) adeguatamente corredata da procedure tecniche esecutive 4. Piano di modifica delle configurazioni ed avviamento del nuovo sistema di rilevamento e gestione incidenti
Benefici	• Maggiore controllo e gestione degli eventi informatici • Diminuzione del rischio di accesso abusivo alle risorse e di manipolazione fraudolenta dei dati

[1] Sono disponibili anche strumenti gratuiti di cifratura per il traffico e i protocolli.

Punti di forza	• Maggiore reattività in caso di incidenti informatici • Minori costi di strumentazione
Punti di debolezza	• Maggiori costi di gestione del parco macchine • Aumento del tempo uomo per le azioni di controllo e verifica
Costi	**Interni**
	• Tempo uomo per lo svolgimento di tutte le attività • Tempo uomo per il monitoraggio periodico degli eventi
	Esterni
	• Affiancamento a supporto delle attività

Soluzione B: Utilizzo di uno strumento di rilevamento delle intrusioni	
Descrizione attività	1. Definizione e stesura di una politica di avviso e allarmistica (alerting e alarming) adeguatamente corredata da procedure tecniche esecutive 2. Identificazione delle regole anti-intrusione necessarie al sistema 3. Definizione e stesura di una politica di gestione degli incidenti (incident handling) adeguatamente corredata da procedure tecniche esecutive 4. Progettazione, installazione e personalizzazione dello strumento di rilevamento delle intrusioni 5. Piano di avviamento del nuovo sistema di rilevamento e gestione incidenti
Benefici	• Elevatissimo controllo e gestione degli eventi informatici • Forte protezione delle risorse e dei dati aziendali • Reazione e protezione automatica ai più comuni tipi di attacco
Punti di forza	• Protezione anche dagli attacchi informatici • Forte protezione dei servizi critici • Elevata reattività in caso di incidenti informatici (anche proattiva e in tempo reale) • Minori costi di gestione del parco macchine
Punti di debolezza	• Costo dello strumento adottato • Tempo uomo per l'amministrazione dello strumento
Costi	**Interni**
	• Tempo uomo per la definizione delle politiche • Tempo uomo per seguire le attività di progetto • Tempo uomo per l'apprendimento dell'uso del nuovo sistema
	Esterni
	• Acquisto e manutenzione dello strumento • Acquisto dell'hardware necessario • Consulenza per la realizzazione del progetto

Parte IV – Macro indicazioni economiche

Ipotesi iniziali:
- 30 server e 300 postazioni utente
- Qualità eccellente
- Documentazione opzionale
- Possibile elevata variabilità delle stime
- Costo al giorno per consulenza dai 450 ai 650€ al giorno

Gestione password

Soluzione A: "Gestione manuale interna"	
Costi	**Interni**
	• Tempo uomo per la definizione delle procedure • Tempo uomo per la sistemazione delle password attuali • Tempo uomo per i controlli futuri • Tempo uomo per le attività di help-desk
	Esterni
	• dai 5 ai 10 giorni (solo affiancamento) + 5 giorni per documentazione

Soluzione B: "Gestione automatizzata delle password"	
Costi	**Interni**
	• Tempo uomo per la definizione delle politiche • Tempo uomo per seguire le attività di progetto • Tempo uomo per l'apprendimento dell'uso del nuovo sistema
	Esterni
	• costo prodotto 3/5000€ + 10 giorni di progetto + 3 giorni per documentazione

Allineamento delle versioni ed applicazione delle patch di sicurezza

Soluzione: "Aggiornamento manuale"	
Costi	**Interni**
	• Tempo uomo per l'analisi dell'esistente • Tempo uomo per la fase di testing e aggiornamento
	Esterni
	• Dai 5 ai 10 giorni + 2 giorni per documentazione

Blindatura e configurazione avanzata delle macchine

Soluzione: "Blindatura manuale"	
Costi	**Interni**
	• Tempo uomo per la definizione delle procedure di blindatura • Tempo uomo per seguire le attività
	Esterni
	• Dai 10 ai 15 giorni + 2 giorni per documentazione (qualche giorno in meno nel caso venga fatta l'attività precedente)

Politica di utilizzo dei documenti e dei dati sensibili

Soluzione: Definizione della politica	
Costi	**Interni**
	• Tempo uomo per la definizione della politica e delle procedure • Tempo uomo per i controlli periodici
	Esterni
	• Dai 3 ai 6 giorni + 3 giorni per documentazione

Protezione dalle agenzie

Soluzione: Studio di fattibilità preliminare	
Costi	**Interni**
	• Tempo uomo per la raccolta iniziale delle informazioni
	Esterni
	• Dai 10 ai 20 giorni + 2 giorni per documentazione

Segmentazione della rete interna

Soluzione: Studio di fattibilità preliminare	
Costi	**Interni**
	• Tempo uomo per la raccolta iniziale delle informazioni
	Esterni
	• Dai 10 ai 20 giorni + 2 giorni per documentazione

Studio corretta configurazione desktop e laptop

Soluzione: Rafforzamento della configurazione delle postazioni	
Costi	**Interni**
	• Tempo uomo per l'analisi e la definizione delle nuove impostazioni • Tempo uomo per l'applicazione di quanto definito
	Esterni
	• Dai 3 ai 6 giorni (solo affiancamento) + 3 giorni per documentazione

Cifratura del traffico, dei protocolli e del database

Soluzione A: Analisi per l'utilizzo della cifratura	
Costi	**Interni**
	• Tempo uomo per seguire le attività di progetto • Tempo uomo per l'apprendimento dell'uso dei nuovi sistemi
	Esterni
	• Eventuale costo di prodotti + 10 giorni di progetto + 3 giorni per documentazione

Controllo e gestione delle intrusioni

Soluzione A: Gestione manuale degli eventi critici	
Costi	**Interni**
	• Tempo uomo per lo svolgimento di tutte le attività • Tempo uomo per il monitoraggio periodico degli eventi
	Esterni
	• Dai 10 ai 20 giorni di progetto + 5 giorni per documentazione

Soluzione B: Utilizzo di uno strumento di rilevamento delle intrusioni	
Costi	**Interni**
	• Tempo uomo per la definizione delle politiche • Tempo uomo per seguire le attività di progetto • Tempo uomo per l'apprendimento dell'uso del nuovo sistema
	Esterni
	• costo prodotto minimo 5.000€ max 30.000 €+ dai 10 ai 15 giorni di progetto + 2 giorni per documentazione