]HackingTeam[

XXXXXXXXX

PHYSICAL ASSESSMENT

Milano

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

]HackingTeam[	

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	02 feb. 2007	Emissione
2.0	05 feb. 2007	Revisione a fronte di feedback del cliente

INFORMAZIONI		
Data di Emissione	05 feb. 2007	
Versione	2.0	
Tipologia Documento	Documento di vulnerability assessment	
Numero di Protocollo	//	
Numero Pagine	40	
Numero Allegati	1	
Descrizione Allegati	1	Evidenze delle attività eseguite
Redatto da	Marco Valleri	
Approvato da	Gianluca Vadruccio	

INDICE

1 Introduzione

Un *vulnerability assessment* ha il compito di identificare le vulnerabilità esposte da un sistema e quantificare l'impatto nel caso queste vulnerabilità possano essere utilizzate per danneggiare il sistema stesso.

Un classico *vulnerability assessment* logico (o *ethical hacking*) analizza le vulnerabilità esposte da un sistema informatico (misconfigurazioni, *bug* delle applicazioni o dei sistemi operativi, cifratura dei dati, etc.) e quantifica il possibile impatto derivante da una sua compromissione: furto o perdita di dati importanti, manipolazione dei processi aziendali, danni all'immagine, etc. Un *vulnerability assessment* di livello fisico, pur nell'ottica di proteggere un sistema dai medesimi rischi, analizza le vulnerabilità presentate dalle "difese fisiche" (sistemi d'accesso, sistemi di rilevazione della presenza, sistemi di protezione dei dati cartacei, etc.) e dagli eventuali sistemi di difesa secondari (sia logici che fisici).

In questo caso, viene simulato l'attacco da parte di figure criminali che possono o tentano di avere un accesso fisico ad un edificio ed alle risorse in esso contenute. Questo accesso può essere ottenuto in maniera illecita (es: tramite effrazione, social engineering, etc.), o in maniera lecita (es: un consulente o un dipendente "malizioso").

Scopo dell'*assessment* è quindi quello di valutare sia i sistemi di difesa che dovrebbero impedire ad un esterno di accedere all'edificio (tornelli, serrature, etc.), sia le infrastrutture e le policy di difesa delle risorse e dei dati sensibili, a fronte di un attacco proveniente da chi è già all'interno dell'edificio, e magari residente in una posizione privilegiata o in possesso di informazioni privilegiate.

Il fenomeno degli attacchi proveniente dagli "insider" è infatti un trend in crescita (83% degli incidenti rilevati nel 2005) e nel 78% dei casi non era stata prevista alcuna policy di sicurezza che vietasse esplicitamente ai colpevoli di compiere le azioni che poi hanno portato al furto o alla frode ("nessuno mi ha detto che non potevo entrare nel CED senza badge….").

E' evidente quindi come sia importante elevare il proprio livello di sicurezza per far fronte ad attacchi di questo tipo, che coinvolgono non solo la componente informatica, ma

anche quella fisica e sociale. Ed è ancora più importante elevare tale livello sia da un punto di vista tecnologico che da un punto di vista organizzativo/procedurale.

2 Struttura del documento

Per meglio evidenziare il reale impatto delle vulnerabilità rilevate, l'importanza della loro interconnessione (es: una vulnerabilità "bassa" da sola è poco importante, due vulnerabilità "basse" combinate insieme possono avere al contrario un grosso impatto) e "chi" e "come" potrebbe compiere un attacco, è importante redigere un documento con una certa attenzione. Il documento è quindi strutturato nel seguente modo:

- Definizione delle aree oggetto di studio, delle metodologie di analisi e delle relative potenziali fonti di vulnerabilità (capitolo 3).
- Elenco dei test effettuati nelle singole aree (capitolo 4).
- Risultati dei test positivi (punti di forza) e negativi (punti di debolezza), corredati da suggerimenti per mitigare ogni vulnerabilità (capitolo 5 e capitolo 6).
- Definizione dei possibili profili di un attaccante (capitolo 7).
- Definizione degli scenari d'attacco (attivi e passivi) con i relativi prerequisiti (riferimento a vulnerabilità sfruttate, *skill* necessari all'attaccante, etc.) e fattori mitiganti (riferimento ai punti di forza); indicazione del possibile impatto di ogni attacco. (capitolo 9)
- Giudizio complessivo con indicazione delle *best practice* da seguire per migliorare il livello di sicurezza generale (capitolo 10 e capitolo 7).

3 Macro-aree di analisi

Il test è stato studiato ed effettuato al fine di dare una visibilità totale sulle problematiche interne di sicurezza del Cliente. La difficoltà di questa analisi, nella sua interpretazione e nella scelta delle soluzioni non è legata alle infrastrutture in quanto tali, ma alle interazioni esistenti tra loro.

All'interno di un'organizzazione bancaria, i livelli nei quali un'informazione sensibile transita sono di differente natura: fisica, logica, digitale. Durante questa transazione interna, le persone e gli strumenti che vi interagiscono possono errare nel comportamento, essere manipolate e, in generale, costituire le vittime di un attacco.

L'approccio suggerito da HackingTeam non consiste nell'analizzare la problematica seguendo la catena di operazioni che un'informazione segue: questo approccio rischierebbe di essere vincolato al funzionamento interno delle strutture xxxxxx allo stato attuale, dando un risultato difficilmente applicabile in futuro. Il report analizza le macro aree di interesse in modo che possano essere seguite da reparti specializzati, dal fisico all'IT, in maniera che ognuno possa intervenire sulla parte di competenza, svincolato dalle funzioni bancarie che vi interagiscono.

Le macro aree indicate non sono strutturate in relazione ad i reparti specializzati in XXXXXXXX, ma sono definite seguendo i campi d'azione nei quali un attaccante può differenziarsi da un altro.

Ognuna delle macro aree rappresentano, metaforicamente, un anello della catena della sicurezza. L'anello più debole rappresenta il livello di sicurezza di tutta la struttura. Per questo motivo, piuttosto che investire sulla massima sicurezza di un elemento, è meglio mantenere tutti gli elementi ad un valido/coerente livello in modo da rendere più difficile l'attacco ad uno spettro più ampio di profili.

3.1 Area fisica

La sicurezza dell'area fisica è conosciuta sin dall'antichità. La sua definizione è di poter verificare che una persona specifica possa accedere a varie zone dell'infrastruttura solo se adeguatamente abilitato. Essa è una delle basi più solide della sicurezza, dal momento che un dato, digitale, fisico, visivo o uditivo può certamente essere compromesso se la locazione fisica nel quale risiede non è protetta.
La sicurezza fisica in un ambiente a rischio come le sedi XXXXXXXX, se compromessa, può consentire ad un attaccante di abusare dei dati legati a quella locazione e transitanti in quella locazione.
La sicurezza fisica deve essere valutata in relazione a vari aspetti, sia autenticativi e d'accesso sia di confinamento delle strutture.
Una serratura può essere forzata e lo sforzo che un attaccante impiega a forzare la serratura sarà il livello di sicurezza di quell'area. L'utilizzo di badge, di tecnologie RFID per l'accesso rappresentano solo un diverso tipo di chiave: elettronico anziché fisico. La sicurezza degli accessi viene innalzata rendendo la procedura di autenticazione più sicura, aumentando ad esempio gli elementi autenticativi (un codice, un'impronta digitale, oltre che ad una chiave fisica o elettronica).
La sicurezza fisica va valutata inoltre su tutto il perimetro, constatando la possibilità di accessi non convenzionali tramite altre vie differenti dalla prevista. La vicinanza ad altri stabili rende più facile l'ingresso di un attaccante tramite finestre o balconi, l'utilizzo di pannelli prefabbricati per la suddivisione delle camere rende possibile uno sfondamento degli stessi.

Ad esempio: il posizionamento di microspie all'interno di una sala riunioni compromette i dati che verranno discussi in quella sede. L'accesso ad una stanza nella quale vengono stampate o scritte informazioni sensibili va consentito esclusivamente a tutti coloro che ne vengono a contatto ed a loro soltanto. L'analisi dell'area di sicurezza fisica valuta la possibilità reale che un attaccante vi acceda.

3.2 Area di profilazione

La profilazione è la rappresentazione in termini di sicurezza delle funzionalità e del lavoro di un collaboratore XXXXXXXX. La profilazione è l'operazione di descrizione di ciò che un collaboratore è abilitato a fare, al fine di potergli assegnare un profilo di appartenenza. Ogni profilo conterrà la descrizione dei permessi legati alle singole aree ed alle operazioni consentite. La profilazione deve essere il più possibile diversificata e granulare (nei limiti della complessità gestionale) e deve consentire la descrizione dei permessi di una persona relativamente a differenti aree di interesse.

La profilazione deve abilitare a privilegi in modo *mandatorio*. Si intende così dire che solamente gli utenti abilitati accedono ad una particolare area, fisica o logica, e nessun altro. Quando viene redatta una politica di profilazione bisogna evitare alcuni errori comuni, come il considerare i privilegi a piramide (l'utente di tipo A ha privilegi X, l'utente di tipo B ha X+Y); raramente infatti è necessario che tra profili differenti ci sia una ridondanza di permessi.

La profilazione deve tener conto della differenza tra un accesso di tipo esecutivo ed un accesso fisico senza permessi ulteriori. Considerando questi elementi discriminanti, il numero di profili realizzabile, senza impattare sull'organizzazione aziendale, diventa sufficientemente grande da poter inquadrare il personale, evitando un grosso numero di operatori dai privilegi elevati in più aree di interesse.

La profilazione deve essere considerata in tutte le aree d'interesse; ai fini della sicurezza informatica, permettere l'accesso fisico dove l'accesso informatico è inibito, significa rendere del tutto inutile la granularità dei privilegi implementata.

Ad esempio: un operatore del call center dovrebbe avere i permessi per accedere solo al piano del call center. Dal momento che nessun altro, ad eccezione di chi svolge operazioni di supervisione e di gestione, dovrebbe poter accedere al call center, a chi svolge altre mansioni sarà inibito l'accesso. Chi svolge operazioni di gestione e supervisione potrà accedere alle stanze del call center, ma non è necessario che abbia i privilegi necessari per accedere all'applicativo di mansione degli operatori.

3.3 Area di confidenzialità ed integrità delle informazioni

Le informazioni che entrano in una catena di elaborazione devono essere protette dall'acquisizione e dalla manipolazione da terze parti. Per confidenzialità si intende la segretezza di un'informazione, e il fatto di non poter essere letta in alcun modo da personale non abilitato. Per integrità invece si intende che non possa essere modificata senza volere durante la sua vita all'interno delle procedure aziendali o al suo transito/permanenza nei sistemi informativi.

Questa area non è legata ad una struttura fisica specifica, ma valuta il trattamento delle informazioni all'interno delle diverse aree. Ciò nonostante, la precauzione e le policy a riguardo non vanno considerate accessorie e ridondanti con quelle dell'area di competenza, poiché le tecnologie di verifica e di controllo non sono vincolate ad una sola area, ma ad un processo.

La confidenzialità e l'integrità vengono assicurate con tecnologie e politiche differenti per obiettivo.

La confidenzialità si ottiene limitando le copie, digitali e cartacee. Devono essere previste tecnologie di cifratura per la diffusione delle informazioni e l'abilitazione alla lettura dei dati solo da aprte degli applicativi e dei profili consentiti.

L'integrità viene anch'essa ottenuta mediante tecnologie di cifratura atte a generare una firma del dato, in modo da poter verificare la sua integrità terminata la catena di elaborazione bancaria, e poter notificare eventuali anomalie.

La verifica d'integrità di un dato andrebbe applicata ad ogni informazione la cui modifica risulta tecnicamente possibile durante la sua esposizione, e qualora la modifica della stessa potrebbe causare problemi.

La segretezza, oltre a meccanismi di protezione dalla lettura, deve prevedere politiche di non diffusione dell'informazione: utilizzo di dispositivi di stampa che rendano più difficile il furto dell'informazione e uso di sistemi di backup appositi in grado di godere di un livello di protezione ulteriore.

Ad esempio: I dati di natura bancaria o legati al cliente, se non adeguatamente protetti, potrebbero essere manomessi durante la loro catena. Si tratta di manomissioni che possono avvenire a svariati livelli: l'amministratore di sistema che modifica il database, un attaccante che intercetta il traffico digitale, personale esterno che falsifica un documento cartaceo al quale si farà riferimento. L'utilizzo e l'affidamento a tecnologie di cifratura/firma supportate da certificati digitali X509 può aiutare ad impedire la modifica in seguito all'apposizione di una firma.

3.4 Area di lavoro e postazione

Una postazione informatica può consentire ad un attaccante di interfacciarsi alla rete con determinate possibilità. Il contenimento fisico dei privilegi, illustrato nelle macro aree precedenti, deve essere applicato anche alle possibilità d'azione di un collaboratore tramite la propria postazione.

Importante è quindi effettuare un'analisi della rete compartimentalizzata, in modo da descrivere politiche d'accesso alla rete differenziate per i differenti profili. In questo modo qualunque sia la tipologia d'attacco scelta dall'attaccante, essa impatterà sulle difese implementate a monte.

Essenziale per limitare attacchi di profilo non altissimo, è il contenimento delle operazioni effettuabile sulle workstation. La compromissione di una workstation molto spesso significa la compromissione del profilo dell'utente, un possibile abuso dei suoi accessi ed una perdita di segretezza delle informazioni a lui accessibili. Impedire attacchi sulle workstation lavorative diventa essenziale in quanto un furto di identità efficace consentirebbe ad un attaccante gli stessi privilegi d'azione della vittima.

Le tecnologie utilizzate all'interno di una workstation classica consentono svariati punti di attacco: inibendo il sistema operativo, togliendo il disco fisso e lavorando su di esso, inserendo *device* esterni ai quali il computer dà priorità ed altre varianti legate allo sviluppo tecnologico. Tuttavia esistono sistemi in grado di proteggere il funzionamento di una workstation dalla sua accensione in poi.

L'utilizzo di questi accorgimenti è necessario per evitare che un collaboratore, senza alcuna strumentazione particolare, possa effettuare furto di dati o manomissione della propria workstation al fine di poter installare applicativi propri.
Oltre che a sistemi di anti-virus ed anti-spyware, indubbiamente utili per evitare che software nocivo alla sicurezza venga installato involontariamente, è consigliabile adottare dei sistemi di contenimento delle operazioni, di verifica dell'integrità delle workstation e di cifratura dei dati persistenti.

Ad esempio: un attaccante in grado di eseguire codice sul computer di una vittima, può prendere il controllo della sua postazione ed avere accesso a quello che al profilo della vittima è consentito. Impedendo attacchi sia fisici che logici si può restringere il campo di azione di un attaccante fino a renderlo non concorrenziale rispetto ad altri attacchi.

4 Test effettuati

Di seguito viene riportata la lista dei test effettuati, suddivisi nelle relative macro-aree. Come da accordi con il cliente, alcuni test non sono volutamente stati effettuati (es: inserimento di microspie, manomissione *paper shredder*, etc.), ma la loro fattibilità è stata valutata e, nei casi ritenuti opportuni, saranno presi in considerazione nella definizione degli scenari d'attacco.

FISICA
Accesso all'edificio Tentativi di accesso all'edificio dagli ingressi convenzionali senza effettuare effrazioni e senza l'utilizzo di *badge* abilitati: • Accesso dall'ingresso principale • Accesso dal garage
Ricerca di accessi alla rete Tentativi di connessione di un *laptop* alla rete del Cliente tramite le porte *ethernet* presenti nell'edificio, sia nelle aree controllate (*open space*, *conference room*, etc.), sia in quelle ad accesso pubblico ("xxxxxxxxxxxx").
Creazione di *rogue access point* Tentativi di creazione di punti d'accesso alla rete interna utilizzabili dall'esterno per effettuare attacchi informatici ("teste di ponte"): • Installazione di Access Point *wireless.* • Installazione di *reverse* VPN.
Clean Desk Policy Verifica della conformità delle postazioni di lavoro e delle aree condivise (armadi, stampanti, etc.) alla *policy* "clean desk": • Cassetti e armadi aperti. • Documenti riservati incustoditi (su scrivanie, stampanti, etc.). • Appunti contenenti dati sensibili, password, etc.

PROFILAZIONE
Accesso ad aree riservate Tentativi d'accesso ad aree riservate dell'edificio senza l'utilizzo di *badge* o con *badge* non abilitati all'accesso in tali aree: • *Patch panels*. • Conference room. • Etc.
Analisi accessi alle aree dati condivise Tentativi d'accesso a risorse in rete (*share*, documenti, e-mail, etc.) non consentite dal profilo utente assegnato per i test: • Global Share. • XXXXXXXX Share. • Etc.
Analisi "internet café" Verifica del corretto funzionamento del filtro alla navigazione nell'area "internet café" e analisi delle possibilità di accesso a internet da parte degli utenti nell'area relax.

CONFIDENZIALITA' E INTEGRITA' DEI DATI
Analisi del traffico di rete Analisi passiva del traffico di rete da una normale postazione di lavoro, alla ricerca di flussi di dati non cifrati e contenenti dati sensibili (password, dati personali, etc.).
Ricerca di *rogue access point* Verifica dell'eventuale presenza di dispositivi senza fili (non autorizzati) che possano permettere l'intercettazione di dati sensibili o l'accesso dall'esterno alla rete del Cliente: • Dispositivi wi-fi (client e AP). • Dispositivi bluetooth (*smartphone*, *headset*, etc.).

POSTAZIONE DI LAVORO

Conformità alle policy

Verifica della conformità delle postazioni di lavoro alle policy XXXXXXXX:

- Privilegi dell'utente.
- Sistemi di sicurezza (*antivirus*, etc.)
- Protezione del *bios.*
- Workstation lock.
- Sistemi antifurto.

Sicurezza logica

Analisi del livello di sicurezza del PC a fronte di attacchi informatici provenienti da altre postazioni e tentativi di manomissione locali:

- Analisi *patch* di sistema.
- Analisi configurazione software.
- Tentativi di *password recovery* locale.

5 Punti di forza riscontrati

Di seguito vengono riportati i risultati dei test di sicurezza che hanno avuto esito positivo e possono quindi essere considerati dei punti di forza dell'infrastruttura di sicurezza fisica e logica del Cliente.

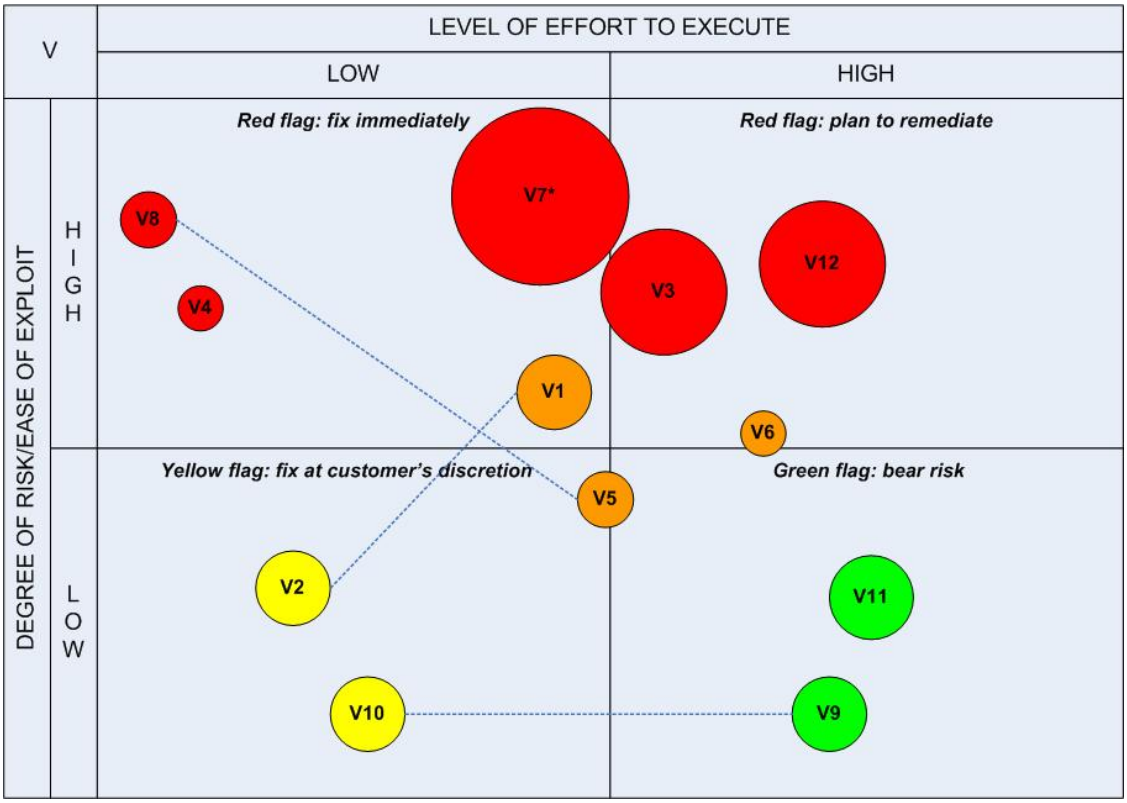
Ogni singolo punto è catalogato tramite un indice che verrà utilizzato come riferimento in fase di definizione degli scenari d'attacco (vedere capitolo 9). All'interno di tali scenari, infatti, i "punti di forza" saranno considerati come fattori mitiganti, in grado quindi di ridurre l'impatto o la probabilità di occorrenza dei vari attacchi ipotizzati.

ID	Punto di Forza
F1	**Sicurezza della postazione di lavoro (laptop)** I test effettuati hanno rilevato una buona sicurezza della postazione di lavoro. Le *security policy* applicate permettono, infatti, di proteggere la postazione da abusi da parte dell'utente (manipolazione dell'OS, avvio da CD, etc.), da furti, e da minacce software provenienti dall'esterno (*malware*, attacchi informatici, etc.). Di seguito vengono elencati i singoli punti che sono stati considerati nella valutazione: • **F1.1 –** *Bios password*, per l'accensione del computer, configurabile dall'utente. • **F1.2 –** Accesso ai parametri di configurazione del *bios* protetto da password non in possesso degli utenti. • **F1.3 –** Impossibilità di avviare la macchina utilizzando media e OS diversi da quelli preimpostati (WindowsXP-SP2 installato su hard-disk). • **F1.4 –** L'utente non è amministratore della propria postazione di lavoro. • **F1.5 –** La postazione è dotata di un sistema *antivirus* aggiornato che è stato in grado di riconoscere ed eliminare alcuni comuni virus utilizzati come test. • **F1.6 –** Utilizzo del sistema *Kensington* con chiave o codice numerico impostabile dall'utente. • **F1.7 –** Il sistema esaminato è risultato aggiornato e non vulnerabile agli attacchi informatici più comuni.

F2	**Buona *password policy* per il *domain* Microsoft** Le *policy* applicate per la gestione delle *password* e della procedura di *login* permettono di proteggere, in maniera adeguata, le utenze del dominio da attacchi di tipo *Password Guessing* o *Brute Force*. Se così non fosse, un attaccante potrebbe essere in grado di elevare i propri privilegi all'interno della rete, impersonare altri utenti, etc. • **F2.1 –** Le password degli utenti devono contenere almeno una lettera maiuscola ed un numero. Questo impedisce all'utente di utilizzare password di banale inferenza. • **F2.2 –** Il sistema di *login* prevede un *lock-out* dell'*account* in seguito ad un certo numero di tentativi di accesso falliti.
F3	**Buon sistema di utilizzo dei *badge*** L'uso di "porta badge" con elastico o cordicella rende difficile il furto o lo smarrimento accidentale delle tessere di riconoscimento. In questo modo, inoltre, il badge risulta comodo da portare sempre con se, e questo riduce notevolmente il numero di tessere lasciate incustodite sulle postazioni di lavoro (nessun badge è stato trovato incustodito durante i sopralluoghi svolti).
F4	**Sistema di rilevazione degli accessi alla rete** Il personale XXXXXXXX è stato in grado di rilevare l'inserimento in rete di un PC laptop non facente parte dell'asset aziendale. La rilevazione non è stata comunque in *real-time*, ma a posteriori (non sarebbe stata in grado di prevenire un intrusione, ma solo di segnalarla), ed è avvenuta una sola volta e da una sola postazione (in seguito a più tentativi d'accesso da postazioni diverse). Sebbene questa rappresenti una nota di merito nella valutazione della sicurezza del cliente, l'utilizzo di sistemi di difesa proattivi (es: *port security* configurato in maniera rigida su tutte le postazioni) è comunque da preferire ai semplici sistemi di rilevazione passivi.

6 Punti di debolezza e vulnerabilità

Le macro-vulnerabilità riscontrate sono raffigurate nello schema di classificazione seguente (rosso: elevata criticità; arancione: media criticità; giallo: bassa criticità; verde: punto di lieve attenzione):



I due quadranti in alto rappresentano le vulnerabilità ritenute critiche: si consiglia di porre rimedio a breve termine per quelle di sinistra (di facile esecuzione); basta invece una pianificazione di copertura per quelle di destra (di difficile esecuzione). Le linee tratteggiate stanno a significare che le vulnerabilità coinvolte sono legate fra loro e che potrebbero essere risolte anche adottando una singola azione di copertura.

La vulnerbailità V7 (evidenziata con un asterisco) non è stata indagata a fondo ma si ritiene molto plausibile che sia effettivamente caratterizzata dal livello di rischio indicato in figura.

Di seguito vengono riportati i risultati dei test di sicurezza che hanno avuto esito negativo, e possono quindi essere considerati dei punti di debolezza o delle vere e proprie vulnerabilità. Ogni singolo punto è catalogato tramite un indice che verrà utilizzato come riferimento in fase di definizione degli scenari d'attacco (vedere capitolo 9).

All'interno di tali scenari, infatti, i "punti di debolezza" e le vulnerabilità saranno considerati come fattori abilitanti, in grado quindi di aumentare l'impatto o la probabilità di occorrenza dei vari attacchi ipotizzati. Inoltre ad ogni debolezza è associato un coefficiente (*Low*, *Medium* o *High*), che indica quanto l'elemento in sé possa contribuire all'attuabilità dei vari scenari.

Unitamente ad ogni punto di debolezza viene anche indicata (dove possibile) quella che HackingTeam ritiene la soluzione più adatta alla realtà del cliente, per eliminare o mitigare la relativa vulnerabilità.

In generale è stata notata una bassa presenza di ***defense in depth***. In altre parole, l'intera sicurezza fisica e logica dell'edificio, della rete, dei sistemi e dei servizi, è affidata, nella maggior parte dei casi, ai sistemi di difesa di primo livello (sistema di controllo accessi dall'ingresso, policy per l'accesso alla rete, etc.); mancano quasi del tutto i sistemi di difesa secondari (es: accesso ad ogni piano tramite badge, *enforcement* del traffico di rete, etc.). In questo modo, se un attaccante è in grado di effettuare il *bypassing* dei sistemi primari (vedi V6), o durante un *failure* casuale degli stessi (come nel caso di V5.1), la sicurezza generale viene messa a rischio.

ID	Risk	Punto di Debolezza
V1	*Medium/ High*	**Accessi alla rete nelle *conference room*** All'interno delle *conference room* esaminate sono state trovati dei cavi di rete a cui è stato possibile collegare un laptop. Dopo aver ottenuto un indirizzo di rete valido (tramite DHCP), è stato possibile accedere all'intera rete interna del Cliente. E' stato quindi provato che è possibile collegare alla rete interna, senza alcuna restrizione o possibilità di controllo, PC che non rispettino le rigide *policy* di sicurezza per le postazioni di lavoro (F1). Il livello di rischio di questa vulnerabilità è incrementato dai punti successivi (in particolare V2, V3 e V6).
V2	*Low/ Medium*	**Scarso controllo delle *conference room*** Le porte delle *conference room* sono aperte per la maggior parte del tempo, anche se le sale sono vuote. Nonostante le pareti di vetro permettano di vedere l'interno delle sale, è stato possibile stazionarvi per circa mezz'ora e utilizzare un laptop collegato in rete, senza alcun intervento di controllo da parte del personale di XXXXXXXX. Questa vulnerabilità aumenta il livello di rischio di V1. E' possibile inoltre supporre che sia possibile posizionare microspie o semplici registratori all'interno delle *conference room*, ed andarli a riprendere, senza che il personale se ne accorga.
V3	*Medium*	**Basso livello di protezione del traffico in rete** La piccola parte della rete esaminata, anche se non specificatamente oggetto dell'*assessment* fisico, ha denotato una scarsa attenzione alla protezione dei dati. La rete è risultata piatta (non suddivisa in VLAN) e il traffico che è stato possibile analizzare, anche contenente dei dati discretamente sensibili, è risultato non cifrato (vedi A.8). Questa vulnerabilità incrementa il livello di rischio di V1.
V4	*High*	**Bassa granularità nella profilatura dell'accesso ai dati condivisi** Il profilo utente utilizzato durante i test avrebbe dovuto avere accesso unicamente all'area dati condivisa "GlobalShare". Utilizzando il medesimo utente è stato però possibile avere accesso anche ad altre aree condivise, contenenti dati discretamente sensibili, in totale violazione del principio di sicurezza del "privilegio minimo". (A.3 – A.7).

V5	*Medium*	**Mancanza di controllo sull'accesso ai piani** Una volta entrati nell'edificio, l'accesso ai vari piani non è regolamentato dall'utilizzo dei *badge,* e non permette di discriminare fra diversi profili. In questo modo, ad esempio, un dipendente del Call Center che si fermi oltre l'orario di lavoro, è in grado di salire ai piani superiori (deserti a quell'ora) ed avere libero accesso alle postazioni di lavoro, ricercare documenti lasciati incustoditi, o addirittura manomettere i computer, rubando o danneggiando dati sensibili, installando *keylogger* fisici[1], etc. Inoltre, le porte di accesso dalle scale ai singoli piani, sebbene dotate di lettore badge RFID, sono risultate aperte per tutta la durata dei test. Il Cliente ha segnalato questa come anomalia momentanea già conosciuta (V5.1).

[1] Semplici apparecchi, comunemente disponibili su internet, che si collegano in maniera quasi invisibile al PC e permettono di registrare tutti le sequenze di tasti battute (es: e-mail, password, etc.). Ovviamente, apparecchi di questo tipo non possono essere individuati utilizzando *antivirus* o altre soluzioni di tipo software.

V6	*Medium*	**Bassa sicurezza dei sistemi di accesso primari** I sistemi di controllo accessi all'edificio possono essere aggirati in maniera discretamente semplice. Nello specifico: • **Accesso dall'ingresso principale (V6.1):** non sono presenti tornelli. Il mancato utilizzo del badge non inibisce l'accesso, ma impedisce di chiamare l'ascensore al piano terra per un tempo di circa un minuto. Camuffando il mancato utilizzo del badge per una disattenzione, è sufficiente attendere che un "collega" scenda al pianterreno, o utilizzi il suo badge e chiami l'ascensore, per accedere all'edificio. Dal momento che le mancate letture dei badge, o le semplici disattenzioni degli utenti legittimi, sono risultate abbastanza comuni, un'attività di questo tipo è passata del tutto inosservata al personale presente. Inoltre, la necessità di attendere un *timeout* prima di poter utilizzare l'ascensore permette di aspettare il "collega" senza destare sospetti. • **Accesso dal garage (V6.2):** La porta che permette di accedere dal garage all'edificio non è munita di lettore badge. E' sufficiente attendere l'apertura del cancello del garage per garantirsi l'accesso al piano -1 del palazzo. Qui l'ascensore necessita del badge per essere utilizzato, ma le porte di accesso alle scale (e ai vari piani, vedi V5.1), essendo risultate aperte, hanno permesso di accedere all'edificio indisturbati (e senza utilizzare alcun badge). Entrambe queste vulnerabilità incrementano notevolmente il livello di rischio di V1 e V5.

V7	*Medium/ High*	**Postazioni di lavoro non conformi alle *policy*** Le postazioni di lavoro fisse (*desktop*) esaminate non sono risultate conformi alle policy di sicurezza. Nello specifico è stata rilevata la possibilità di effettuare il *boot* da CD e di accedere ai parametri di configurazione del *bios.* Inoltre è stato rilevato come tutte le postazioni di lavoro esaminate abbiano due utenti di sistema in comune (xpguru e xpsupport). E' possibile ipotizzare che le password di questi utenti siano le stesse su tutte le macchine[2]; inoltre, sulle postazioni esaminate, questi utenti avevano privilegi amministrativi. Effettuando il boot da CD, è stato possibile utilizzare dei tool di *password recovery* locale. Con le credenziali così ottenute un attaccante sarebbe in grado di accedere a livello amministrativo a tutte le postazioni in rete che condividono le due utenze sopra citate. E' importante notare come l'accesso da remoto a livello amministrativo permette di monitorare completamente l'attività di qualsiasi utente (es: e-mail, password, documenti riservati, etc.). Va infine sottolineato come la postazione di lavoro laptop fornita per i test non prevedesse la richiesta di password in seguito all'avvio dello *screen saver* (come previsto dalle policy).
V8	*High*	**Non conformità alla policy "clean desk"** E' stato possibile rilevare come, soprattutto nei piani 2 e 5, le postazioni di lavoro (scrivanie, cassetti, armadi) non siano conformi alla policy "clean desk" fuori dall'orario di lavoro. Nello specifico sono stati trovati armadi e cassetti aperti, documenti abbandonati sulle scrivanie o nelle stampanti etc. Parte del materiale rinvenuto conteneva anche dati ritenuti sensibili. Il livello di rischio di questa vulnerabilità è aggravato da V5 e V6.
V9	*Low*	**Filtro navigazione "internet cafe" aggirabile** E' possibile aggirare il *filtering* dei contenuti web nell'area "internet cafe" ed accedere a siti dal contenuto sconveniente (es: porno, etc.).
V10	*Low*	**Mancato controllo d'ingresso hardware** Le policy non prevedono il controllo dell'hardware introdotto nell'edificio (es: laptop dei consulenti). Questo può aumentare il livello di rischio di V1.

[2] Per motivi di privacy non è stato possibile verificare tale ipotesi.

V11	*Low*	**Dispositivi wi-fi e bluetooth** E' stata rilevata la potenziale[3] presenza di *AccesPoint* wireless e dispositivi BT non protetti. E' stata inoltre verificata la possibilità di agganciare, alla rete interna, un dispositivo *wireless* AP che potesse essere utilizzato dall'esterno come "testa di ponte", per effettuare attacchi informatici alla rete interna senza controllo e aggirando le difese perimetrali (firewall, proxy, etc.). Il livello di rischio di questa vulnerabilità è aumentato da V10. I test *wireless* sono stati effettuati ispezionando l'edificio, su tutti i piani, con antenne ed apparati appositi. E' importante sottolineare come sia stato possibile aggirarsi per l'edificio in questo modo, senza badge in vista, e senza attirare l'attenzione del personale.
V12	*Medium*	**Problema traffico "webtop"** Per un problema di configurazione del *cluster* che ospita l'applicazione webtop, il traffico di rete indirizzato verso di essa viene replicato su tutte le porte di tutti i segmenti di rete. Questo rende possibile l'intercettazione, da qualsiasi postazione, del traffico effettuato dai client del Call Center verso il server (vedere A.8), ed anche del traffico fra il server e le potenziali altre macchine coinvolte nel flusso applicativo (es: database). La medesima misconfigurazione permette inoltre di effettuare un attacco di tipo *Denial of Service* che, tramite l'invio di un singolo pacchetto, è in grado di bloccare l'operatività di tutte le postazioni del Call Center che accedono al server webtop.

[3] Non è stato possibile determinare con certezza se il segnale provenisse dall'interno dell'edificio o da uno degli appartamenti adiacenti.

Di seguito viene presentata una tabella riassuntiva delle soluzioni proposte per le singole vulnerabilità riscontrate.

ID	Soluzione proposta
V1	Si consiglia l'utilizzo di sistemi di discriminazione degli accessi (802.1x, *Port Security*, etc.) per tutti i punti d'accesso alla rete situati in zone non strettamente controllate (es: *conference room*). E' inoltre auspicabile che tali punti d'accesso vengano convogliati all'interno di VLAN differenti, da cui sia possibile avere visibilità solo dei sistemi e dei servizi strettamente necessari (ad esempio, un laptop collegato alla rete da una *conference room* potrà navigare sul web, ma non accedere all'applicazione destinata al CallCenter).
V2	Utilizzare del personale per custodire le chiavi delle *conference room*, e per aprirle e chiuderle solo prima e dopo le riunioni. Questa *policy* viene probabilmente già utilizzata per la *meeting room* posizionata al quinto piano.
V3	Si consiglia di suddividere la rete, tramite VLAN, per aree di criticità (isolando ad esempio i segmenti di rete relativi alle *conference room* e al *call center*). Si consiglia inoltre di utilizzare dei canali cifrati per la protezioni dei flussi di dati contenenti informazioni sensibili.
V4	Utilizzare una suddivisione dei privilegi più granulare, in modo che ogni singolo profilo possa accedere unicamente ai dati strettamente necessari alla sua operatività. Per fare questo è necessario intervenire sulle utenze di dominio, aumentando il numero di gruppi e modificando di conseguenza le ACL sui singoli *share*.
V5	La planimetria dell'edificio non consente di inserire, in maniera semplice, dei sistemi di controllo d'accesso (non presidiati) sui singoli piani. Per eliminare questa vulnerabilità sarebbe infatti necessario l'inserimento di porte con *badge* fra gli ascensori e i singoli piani.
V6	Per mitigare questa vulnerabilità senza modificare il sistema di controllo accessi, è necessario aumentare la *security awareness* del personale XXXXXXXX, in particolar modo quello preposto al presidio dell'ingresso. Nello specifico, prevedere ad esempio una verifica del *badge*, da parte del personale, ogni qualvolta il sistema di controllo accessi rileva un ingresso non autorizzato.
V7	Disabilitare il *boot* da CD-ROM e proteggere l'accesso ai parametri di configurazione del *bios* per tutte le postazioni (anche quelle fisse).

V9	Per eliminare totalmente il problema sarebbe necessario restringere drasticamente l'accesso a internet, permettendo la navigazione solo verso determinati siti autorizzati.
V10	Si consiglia di effettuare un censimento, all'ingresso, dell'hardware introdotto all'interno dell'edificio da personale esterno (es: consulenti).
V11	Questa vulnerabilità può essere mitigata notevolmente applicando i *fix* per V1, V3 e V10.
V12	Modificare la configurazione del *cluster* in maniera che le singole schede inviino pacchetti con MAC Address sorgente uguale a quello annunciato nelle ARP Reply. Sarebbe possibile dare indicazioni tecniche più specifiche solo dopo aver esaminato la configurazione attuale del *cluster* e del segmento di rete che lo ospita.

7 Security Plan

Di seguito viene riportata la scaletta degli interventi consigliati da Hacking Team (per una lista completa vedere il capitolo 6) per migliorare il livello di sicurezza offerto dalle policy e dall'infrastruttura di sicurezza del Cliente, e per sopperire alle vulnerabilità riscontrate durante i test, minimizzando di fatto l'impatto e la probabilità di occorrenza degli scenari d'attacco ipotizzati nel capitolo 9. Gli interventi sono elencati in ordine di importanza, partendo da quelli che sono considerati più semplici ed immediati da realizzare, e che maggiormente impattano sul livello di sicurezza generale.

Step	Actions	Coverage
1	Richiedere, al personale preposto, un livello di *security awareness* più elevato e una maggiore conformità alle *policy* di sicurezza (es: "clean desk").	V6 V8
2	Utilizzare del personale per custodire le chiavi delle *conference room*, e per aprirle e chiuderle solo prima e dopo le riunioni. Questa *policy* viene probabilmente già utilizzata per la *meeting room* posizionata al quinto piano.	V2
3	Utilizzare una suddivisione dei privilegi più granulare per gli utenti del dominio che accedono alle risorse condivise, in modo che ogni singolo profilo possa accedere unicamente ai dati strettamente necessari alla sua operatività.	V4
4	Disabilitare il *boot* da CD-ROM e proteggere l'accesso ai parametri di configurazione del *bios* per tutte le postazioni (anche quelle fisse).	V7
5	Modificare la configurazione del *cluster* WebTop in maniera che le singole schede inviino pacchetti con MAC Address sorgente uguale a quello annunciato nelle ARP Reply. Sarebbe possibile dare indicazioni tecniche più specifiche solo dopo aver esaminato la configurazione attuale del *cluster* e del segmento di rete che lo ospita.	V12

6	Si consiglia di suddividere la rete, tramite VLAN, per aree di criticità (isolando ad esempio i segmenti di rete relativi alle *conference room* e al *call center*). Si consiglia inoltre di utilizzare dei canali cifrati per la protezioni dei flussi di dati contenenti informazioni sensibili.	V1 V3 V11

8 Profilatura dell'attaccante

Al fine di contestualizzare gli scenari d'attacco, vanno analizzate delle figure ipotetiche di attaccanti, con *skills* e finalità differenti.

Gli attacchi oltre che a differenziarsi per profilo, per debolezze sfruttate e per resistenze incontrate, si divideranno in attacchi attivi e passivi. I profili indicati cercano di coprire differenti macro aree di interesse e differenti motivazioni.

A1 – Attaccante/spia professionista con finalità di spionaggio (informatico e fisico)

Descrizione: Attaccante professionista al quale viene richiesto di compiere azioni con conseguente danno a sfavore di XXXXXXXX.

Skills: Anni di esperienza in infrastrutture IT, attacchi alle strutture fisiche, informatiche ed umane (social engineering). L'attaccante ha una fotografia completa del funzionamento del sistema bancario, conosce i dati che sta cercando e le strutture che li gestiscono.

Strumentazione in suo possesso: Sistemi informatici in grado di simulare e studiare gli applicativi ed i sistemi operativi. Tools di attacco pubblici o acquisibili con una spesa bassa (valore di un *trojan horse* non riconosciuto dagli antivirus)

Strategia a lungo termine: Essere infiltrato all'interno della struttura con un ruolo al quale non può essere imputata una possibile colpevolezza. Essere infiltrato in un ruolo in cui non sono richiesti skills particolari, che sappia sostenere la sua posizione per un discreto periodo di tempo in modo da eseguire un adeguato raccoglimento di informazioni prima dell'attacco vero e proprio.

A2 – Attaccante improvvisato con finalità di danno

Descrizione: Tecnico XXXXXXXX, offeso o deluso, mosso da sentimenti di vendetta.

Skills: Anni di esperienza sull'infrastruttura di competenza, conoscenza dell'infrastruttura XXXXXXXX, conoscenza/fiducia parziale da parte dei colleghi.

Strumentazione in suo possesso: Strumenti gratuitamente reperibili in rete, computer desktop a casa e workstation lavorativa.

Strategia a lungo termine: Causare una perdita di immagine ad XXXXXXXX, furto di denaro o attacchi al sistema finanziario della banca.

A3 – Spia con finalità di intelligence investigativa/concorrenziale

Descrizione: Spia con anni di esperienza viene assoldata per mettere il proprio datore di lavoro a conoscenza delle strategia di XXXXXXXX.

Skills: Esperienza di infiltrazione e di utilizzo strumenti di penetrazione fisica d'alto livello. Conoscenza delle infrastrutture finanziare in modo generico.

Strumentazione in suo possesso: Strumentazione investigativa clandestina (microspie, splitter informativi) dal valore imprecisato.

Strategia a lungo termine: Tenere sotto controllo le decisioni manageriali e strategiche di XXXXXXXX.

9 Definizione degli scenari d'attacco

Di seguito vengono presentati alcuni scenari d'attacco che, in seguito all'analisi svolta, risultano plausibilmente perpetrabili ai danni del Cliente. Per ogni scenario viene indicato:

- il profilo di attaccante (skills, determinazione, attrezzatura) che potrebbe portarlo a compimento
- quali delle vulnerabilità riscontrate ne permettono/facilitano l'esecuzione
- quali "punti di forza" ne diminuiscono l'impatto o la probabilità di occorrenza.

Gli scenari sono inoltre classificati come:

- **Attivo:** l'attaccante effettua operazioni esplicitamente illecite (es: effrazioni, manomissioni, etc.). Questo tipo di attacco risulta più efficace nell'immediato, ma può essere più facilmente rilevato sia durante la sua esecuzione (es: telecamere, antifurto, etc.), sia a posteriori (es: rilevazione tracce di manomissione).
- **Passivo:** L'attaccante si limita a raccogliere informazioni e dati in modo passivo, senza violare esplicitamente alcuna *policy* o legge, ma sfruttando unicamente punti di *information leaking* (vedere ad esempio V8 e V12). I dati così ottenuti potranno poi essere utilizzati a lungo termine per scopi illeciti. Questo tipo di attacco è generalmente meno efficace del precedente, ma molto difficile da individuare anche a posteriori.

Per i singoli scenari non verrà presentata una valutazione della **probabilità d'occorrenza**, in quanto questa è **legata principalmente alla potenziale volontà di un attaccante** corrispondente ad uno dei profili elencati.

Inoltre, l'impatto di ogni singolo scenario verrà descritto solo in termini oggettivi, lasciando al cliente la valutazione della sua reale pericolosità nell'ottica del suo business.

Scenario 1

Tipologia d'attacco: Attivo

Profilo: A1

Vulnerabilità sfruttate: V5, V3, V11

Fattori mitiganti: F4

Descrizione dell'attacco: Un collaboratore del call-center, che ha seguito da circa un mese il corso formativo ed ha avuto il tempo necessario per adattarsi all'ambiente, vuole impadronirsi di dati sensibili (i clienti ed il loro comportamento finanziario) in quanto assoldato da una banca concorrente. In un mese di tempo, grazie ad una buona capacità sociale viene a conoscenza degli altri piani di lavoro e delle aree di interesse. A volte simula malfunzionamenti della workstation, in modo da analizzare le procedure correttive e conoscere sistemisti e programmatori. Un venerdì pomeriggio termina il suo turno e si attarda nella sala fumatori; tra un caffè ed una sigaretta verifica lo svuotamento progressivo dell'edificio. Nei piani 2, 4 e 5 posiziona un access point con sistema operativo e minidisk integrato in configurazione *bridge ethernet*. Nasconde questi strumenti all'interno dei pozzetti dai quali le stampanti ricevono le informazioni via rete. Gli apparecchi intercettano il traffico ed in modo trasparente lo inviano alla stampante, senza causare alcun disservizio. La notte l'attaccante si collega via wi-fi e scarica i dati intercettati durante il giorno.

Dopo aver nascosto gli access point inserisce anche dei *keylogger* fisici alle postazioni degli amministratori e lascia lo stabile.

Dopo una settimana ha raccolto tutte le password degli amministratori. Avvia un sistema operativo differente dallo standard sulla propria postazione e si collega ad i database interni impadronendosi dei dati.

Eventualmente, manomette i sistemi di distruzione dei documenti allentando o danneggiando le lame. In questo modo i documenti verranno semplicemente piegati e buttati interi all'interno del sacco. Effettua una pulizia degli strumenti la sera precedente al furto. Il giorno seguente si presenta al lavoro e così nella settimana successiva,

recupera gli access point nascosti, danneggia irrimediabilmente gli strumenti di distruzione cartacea e si dimette.

Impatto: Furto di informazioni molto sensibili per XXXXXXXX (sia prodotte in digitale che in cartaceo). Possibile riutilizzo delle informazioni per spionaggio industriale, furto, danno all'immagine, etc.

Scenario 2

Tipologia d'attacco: Passivo

Profilo: A1

Vulnerabilità sfruttata: V12, V7, V8

Fattori mitiganti: F1.2, F1.3, F1.4

Descrizione dell'attacco: Un collaboratore del call-center, che ha seguito da circa un mese il corso formativo ed ha avuto il tempo necessario per adattarsi all'ambiente, ha come finalità di impadronirsi dei dati sensibili (i clienti ed il loro comportamento finanziario) in quanto assoldato da una banca concorrente. Conosce la buona fama di XXXXXXXX per la sicurezza e teme di incappare in sistemi di rilevazione informatica attivi che lo smaschererebbero. Per questo non intraprende alcun genere di attacco informatico via rete. Decide di optare per un attacco passivo, effettuando il minor numero di operazioni invasive all'interno dell'infrastruttura. Analizza la postazione in suo possesso e tramite *password recovery* ne prende il controllo. Installa un software che opera di nascosto per analizzare quello che transita sulla rete, si impadronisce del traffico del call center, suo e di altri utenti. All'interno di questo traffico trova informazioni di parecchi utenti. In seguito alla compromissione della propria postazione, recupera analizzando in separata sede le password cifrate degli utenti amministratori locali della sua macchina. Tramite la postazione compromessa prende il controllo delle postazioni in possesso di *marketing* e *finance*. All'interno di esse individua i dati degli utenti, li scarica sulla propria postazione e tramite chiavetta USB inizia il furto.

La sera, ad orari nei quali difficilmente ci sono impiegati, passeggia tra i piani con uno zaino, riempiendolo fogli contenenti dati sensibili dei clienti. Dopo una settimana dalla rivendita delle sue informazioni e dopo il ripristino del corretto funzionamento della *propria* macchina, si licenzia.

Impatto: Perdita di informazioni sensibili da parte di XXXXXXXX, profilazione finanziaria degli utenti in mano ad i concorrenti.

Scenario 3

Tipologia d'attacco: Attivo

Profilo: A2

Vulnerabilità sfruttata: V4

Fattori mitiganti: F2

Descrizione dell'attacco: Un collaboratore o dipendente XXXXXXXX è particolarmente offeso da qualche avvenimento che giudica sbagliato nei suoi confronti. In alternativa il profilo può essere di tipo terrorista-anticapitalista-insurrezionalista, nelle vesti di una persona già infiltrata da parecchio tempo nella banca, ma senza una grande conoscenza di intrusioni o di spionaggio.

Mentre naviga negli share di rete, inizia ad acquisire tutte le informazioni riservate disponibili in rete, tra le quali tutti i progetti XXXXXXXX, informazioni sugli utenti in file excel protetti da password (facilmente superabili con software gratuiti), informazioni sul personale e mail private. Salva i dati su una chiave USB.

La sera, tramite internet point si registra a dei blog e siti web gratuiti, sui quali pubblica le informazioni XXXXXXXX. I servizi sono scelti in differenti stati con i quali l'Italia non gode di particolari privilegi diplomatici. Le informazioni vengono ridondate, per essere certo che siano più difficilmente oscurabili.

Dalla stessa postazione, invia dei messaggi alle maggiori testate giornalistiche, giornali indipendenti, mailing list e newsgroup pubblici. Informando così della fuga d'informazione in modo rapido.

Il giorno seguente, in ufficio, si gode la vendetta.

Non pago, la sera in un altro internet point sfrutta dei sistemi gratuiti per contattare tutti i clienti XXXXXXXX (dei quali ha l'indirizzo tramite XXXXXXXXShare), con una mail che recita pressappoco:

Gentile (nome e cognome del cliente), Oggi alcune testate giornalistiche hanno attaccato il nostro servizio, sottointendendo un furto di dati dalla nostra Banca.

Vogliamo personalmente smentire questa informazione, i nostri sistemi informativi sono mantenuti sotto costante verifica al fine di proteggere i Vostri dati.

Affinchè mitigare ogni preoccupazione dei nostri clienti, vi proponiamo l'utilizzo di un programma atto a rinforzare i certificati che proteggono i vostri computer.

Allegata a questa e-mail trovate l'eseguibile XXXXXXXXsicuro.exe, avviatelo sulle postazioni dalle quali vi connettete al nostro servizio, godrete così di un'ulteriore verifica.

Grazie

Il binario allegato distrugge i file di documento, fogli di calcolo ed e-mail dei clienti. Una volta fatto lo comunica all'utente.

Impatto: Perdita di informazioni sensibili, pubblica notifica dell'accaduto. Caduta dei titolo XXXXXXXX, perdita di fiducia da parte degli utenti. Articoli diffamatori riguardo lo sfruttamento della fiducia data dagli utenti vittime di un "virus" che ha distrutto loro i dati.

Scenario 4

Tipologia d'attacco: Attivo

Profilo: A3

Vulnerabilità sfruttata: V6, V5, V2, V8

Fattori mitiganti: F3

Descrizione dell'attacco: L'attaccante è stato assoldato con la massima urgenza da alcuni concorrenti bancari, al fine di monitorare le scelte strategiche dirigenziali. L'attaccante è a conoscenza del luogo, alcuni ex collaboratori hanno raccontato le suddivisioni a grandi linee. Una volta fatto un sopralluogo in Spazio Arancio e compreso come si presentano i badge consulente, ne crea uno simile e tenta di entrare alla fine della pausa pranzo. L'allarme suona, cammina in avanti scusandosi con l'accumulo di persone che si sta creando. Sale al piano del call center ed entra in sala fumatori. Rimane a leggere il giornale e dopo qualche ora passa alla sala fumatori del piano successivo, in seguito alla sala fumatori dell'ultimo piano. Verso le 19, notificato che non c'è praticamente più nessuno, nasconde delle microspie tra le piante, nelle torrette, sotto i tavoli delle conference room. Apre alcuni armadi all'interno degli uffici dirigenziali alla ricerca di informazioni. La sala conferenze utilizzata dal consiglio d'amministratore viene appositamente aperta scassinando la serratura.

Impatto: Dal giorno successivo, ogni discussione tenuta all'interno delle sale riunioni del piano dirigenziale, è conosciuta in tempo reale dall'attaccante e da chi l'ha assoldato.

10 Considerazioni conclusive

L'attività di *physical assessment* svolta ha evidenziato un buon livello di attenzione alle tematiche di *security* (fisica e logica) da parte degli "addetti ai lavori" della società cliente. E' possibile rilevare la tendenza alla sicurezza già nel nutrito gruppo di policy già presenti. Di contro, però, in alcuni casi queste policy risultano non applicate o applicate in maniera troppo "leggera", probabilmente a causa dell'ambiente a volte "troppo" informale e del personale "generico" poco *security aware* (tranne in alcuni casi sporadici).

Oltre alle debolezze introdotte dal "fattore umano", considerato da sempre l'anello debole nella catena della sicurezza, è stata notata, in generale, una bassa presenza di ***defense in depth***. In altre parole, l'intera sicurezza fisica e logica dell'edificio, della rete, dei sistemi e dei servizi, è affidata, nella maggior parte dei casi, ai sistemi di difesa di primo livello (sistema di controllo accessi dall'ingresso, policy per l'accesso alla rete, etc.). Mancano quasi del tutto i sistemi di difesa secondari (es: accesso ad ogni piano tramite badge, *enforcement* del traffico di rete, etc.). In questo modo, se un attaccante è in grado di effettuare il *bypassXXXXXXXX* dei sistemi primari (vedi V6), o durante un *failure* casuale degli stessi (come nel caso di V5.1), la sicurezza generale viene messa a rischio, ed i possibili impatti vanno dal furto di dati sensibili (a fini di spionaggio o di lucro), al danno (blocco o manomissione di un servizio), alla perdita d'immagine.

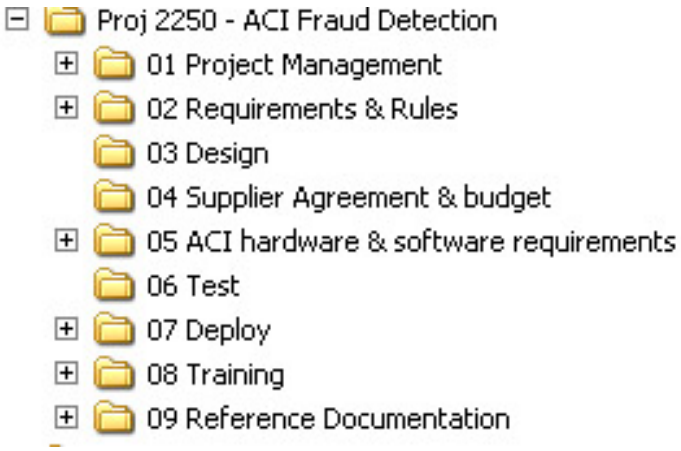
In questo contesto, la fattibilità di un attacco (sul modello di quelli elencati nel capitolo 9) è legata principalmente alla determinazione di un attaccante e al suo livello di *skill*. In generale, è impossibile azzerare totalmente la probabilità di occorrenza di simili attacchi, ma è possibile utilizzare una serie di accorgimenti per innalzare la soglia di *skill* e di determinazione necessari per portarli a termine. Alcuni di questi "accorgimenti" sono semplici da implementare e poco impattanti sull'infrastruttura fisica e logica del Cliente (vedere il capitolo 7), e permettono di innalzare notevolmente il livello di sicurezza generale. D'altra parte, alcuni degli scenari d'attacco sono resi possibili dalla mancanza

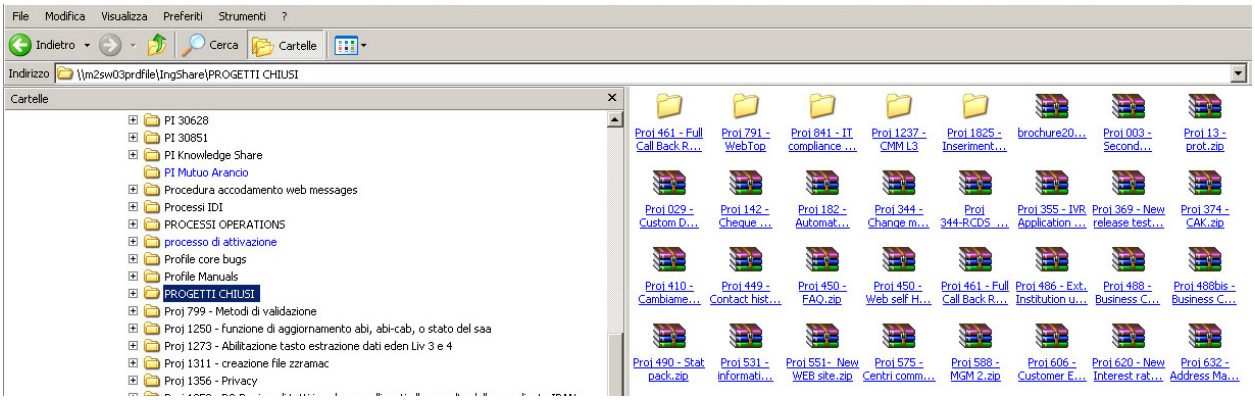
di discriminazioni d'accesso ai singoli piani dell'edificio (es: un dipendente del call center può salire al piano del management e aggirarsi negli spazi comuni). Per far fronte a questo problema non è possibile ipotizzare soluzioni semplici (a meno di modifiche strutturali nell'edificio, con l'inserimento di porte, lettori di badge all'intero dell'ascensore, etc.); al contrario è necessario innalzare gli altri livelli di difesa (es: clean desk policy) e arginare il problema considerando tutti gli spazi comuni come zone *untrusted*.

ALLEGATO 1 – Evidenze dell'attività

Di seguito vengono elencati degli estratti di alcuni dei documenti che è stato possibile reperire tramite l'accesso ad alcune aree dati condivise.

A.1 – Progetti chiusi visibili in XXXXXXXXShare





A.2 – Script di posta visibili in GlobalShare

A.3 – Codice per la cifratura/decifratura del PIN (EncryptionPIN.zip)

```
Private Const gv_sAnalyse = "111111"

Public Function DecryptPIN(ByVal strPin As String) As String
    Dim strDecPin As String * 256
    Dim intLen As Integer

    Analyse gv_sAnalyse
    intLen = Dec(strPin, strDecPin)
    DecryptPIN = Left(strDecPin, intLen)
End Function
Public Function EncryptPIN(ByVal strPin As String) As String
    Dim strEncPin As String * 256
    Dim intLen As Integer

    Analyse gv_sAnalyse
    intLen = Enc(strPin, strEncPin)
    EncryptPIN = Left(strEncPin, intLen)
End Function
```

A.4 - Datadump.xls

IdPratica	Originator	ChiaveBanca	Finalita	Importo
9304	Lb. MOL	xxxx	XXXXXXXXxxxxxxxx	50000
9306	Lb. MOL		XXXXXXXXxxxxxxxx	100000
9468	Call center XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	368000
9578	Call center XXXXXXXX	xxxx 1	XXXXXXXXxxxxxxxx	160000
9579	Call center XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	140000
10621	Lb. MOL		XXXXXXXXxxxxxxxx	164000
11445	Sito XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	368000
11446	Sito XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	100000
11447	Sito XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	300000
11468	Sito XXXXXXXX		XXXXXXXXxxxxxxxx	120000
11536	Lb. MOL		XXXXXXXXxxxxxxxx	100000
11616	Sito XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	80000
11648	Call center XXXXXXXX		XXXXXXXXxxxxxxxx	80000
11649	Sito XXXXXXXX		XXXXXXXXxxxxxxxx	100000
11650	Sito XXXXXXXX		XXXXXXXXxxxxxxxx	100000
11651	Sito XXXXXXXX		XXXXXXXXxxxxxxxx	120000
11655	Call center XXXXXXXX	xxxx	XXXXXXXXxxxxxxxx	100000

A.5 – Database Access AssegniCircolari.mdb

Con riferimenti a nomi, date, importi, conti.

A.6 – Utenze UAT con password

A.7 – Log AWAYA

Session=448e715b000300000a71ca771b590002

Request=448e715b000400000a71ca771b590002

A.8 – Dump traffico WebTop

```
..XXXXXXXXCExtAccounts.GetExtAccounts|.3.00200146408DI17 U37069573091R790
6|0||1|1|18|||1.0200801009.000003225882
```