SECURITY RATING – LO SCENARIO

La maggior parte delle attività legate al business aziendale si sono ormai da tempo spostate sul Web ed in generale sulle connessioni Internet e Mobile. Questo ha contribuito alla nascita di organizzazioni criminali che sfruttano questa evoluzione rubando dati ed attaccando quelle realtà che non hanno adottato adeguate contromisure di sicurezza. Per raggiungere il loro scopo, quasi esclusivamente legato a fattori economici, le cyber gang utilizzano tutti i mezzi, compreso l'utilizzare le relazioni informatiche che le società hanno con partner e fornitori esterni, ovvero con le terze-parti.

Anche i clienti si sono adeguati ai tempi e non vogliono avere a che fare con realtà che non proteggono adeguatamente i loro dati o i cui servizi non sono resi sicuri dai pirati informatici. Ad esempio, il 57% dei fruitori di un sito web si rivolge ad altri se le pagine non si visualizzano entro 3 secondi!

Vi affidereste ad una società che si è lasciata rubare i dati dei propri clienti? Continuereste ad usufruire di un servizio costantemente lento o non disponibile?

La reputazione in termini di sicurezza di una società è diventata fondamentale per il business stesso. Per mantenere alta tale reputazione occorre:

- pensare seriamente alla propria sicurezza,
- valutare attentamente la sicurezza delle proprie terze parti.

La capacità di valutare il proprio rating di sicurezza in modo semplice, affidabile ed oggettivo, per sé stessi e per i propri potenziali partner/fornitori, è un'abilità cruciale nel mondo moderno. Il servizio erogato da Xecurity permette di valutare tale reputazione e di eseguire un assessment quantitativo e preciso del livello di Rischio informatico della propria organizzazione e delle proprie terze parti. Per tali problematiche Xecurity propone un approccio costituito da due punti cardine:

1. ASSOLUTA NON INTRUSIVITA': il servizio è completamente non intrusivo sul cliente e sul suo sistema informativo. I dati oggetto dell'analisi vengono raccolti esclusivamente dalla rete Internet e nulla viene installato o rilevato nell'infrastruttura del cliente.
2. ORIENTATO AI DATI PUBBLICI. I dati sono raccolti sia da vari repository internet, pubblici o ad accesso privato, sia dal traffico che transita sulla rete. Le successive analisi, correlazioni, sintesi, report di tali dati costituiscono il fulcro del servizio offerto.

QUALI SONO I CRITERI CON CUI SCELGO I MIEI FORNITORI?

Valutare la sicurezza dei miei fornitori è fondamentale affinché loro stessi non costituiscano un veicolo di potenziali minacce verso il mio sistema informativo, i miei servizi, i miei dati, il mio business.

POSSO FIDARMI DEI MIEI PARTNER?

Fra i maggiori furti di dati accaduti del 2015 e del 2016 hanno potuto essere condotti con successo grazie alla scarsa sicurezza delle terze parti collegate informaticamente al vero target.

COME POSSO MISURARE IL MIO LIVELLO DI SICUREZZA E DI RISCHIO?

Oltre alla valutazione quantitativa ed oggettiva del proprio livello di rischio è corretto e importante misurare il proprio rating di sicurezza e compararlo a quello dei miei competitor o, più in generale, con quello del mio settore merceologico di riferimento.

XECURITY S.R.L.
VIA GALLARATE, 156
20151 MILANO
WWW.XECURITY.IT

SECURITY RATING – L'APPROCCIO

Il servizio di misurazione del rating di sicurezza e del conseguente livello di rischio informatico offerto da Xecurity si basa sui punteggi ottenuti dalla analisi e valutazione di 3 macro tipologie di elementi:

1. COMPROMISSIONE: rilevamento di eventi che potrebbero indicare una possibile infezione o un possibile attacco già avvenuto con successo,
2. DIFESA: la verifica dell'attuazione diligente, da parte della realtà esaminata, di quelle attività relative alla minimizzazione dei rischi,
3. ACCADIMENTO: la constatazione di eventi malevoli già accaduti.

COMPROMISSIONE

Gli eventi portatori di rischio rappresentano la parte delle valutazioni che maggiormente pesa sul Rating finale. Sono tutti quegli eventi osservati sulla rete che indicano un rischio di compromissione dell'infrastruttura dell'azienda. Sono raggruppati in cinque tipologie:

1 a. Infezioni: rilevamento di pc e server compromessi.
1 b. Propagazione di spam: identificazione di macchine che inviano all'esterno email di spam.
1 c. Malware: rilevamento di server che ospitano attività malevoli quali phishing, scamming…
1 d. Potenzialmente compromessi: verifica di macchine che ospitano Adware, ovvero malware pubblicitario non pericoloso ma che indica un computer infetto e quindi rischioso.
1 e. Contatti insoliti: rilevamento di comunicazioni verso l'esterno non previste o verso indirizzi esterni non usuali.

DIFESA

Questi eventi sono quelli che dimostrano le azioni che diligentemente un'azienda ha intrapreso per minimizzare i rischi di infezione. Rappresentano la parte positiva e proattiva dell'analisi. Sono raggruppati in quattro tipologie:

3 a. Utilizzo di SPF, ovvero la corretta identificazione e gestione dei server di posta autorizzati a inviare email per conto di un certo dominio.
3 b. Utilizzo DKIM, ovvero quella corretta impostazione crittografica che impedisce ad un server di spedire posta per un certo dominio se non autorizzato.
3 c. Utilizzo SSL: viene controllata la forza dei certificati SSL utilizzati; validità, appartenenza ad una CA autorevole, forza crittografica e vulnerabilità del protocollo.
3 d. Utilizzo DNSSEC, ovvero di quel protocollo crittografico che assicura l'autenticità e l'integrità

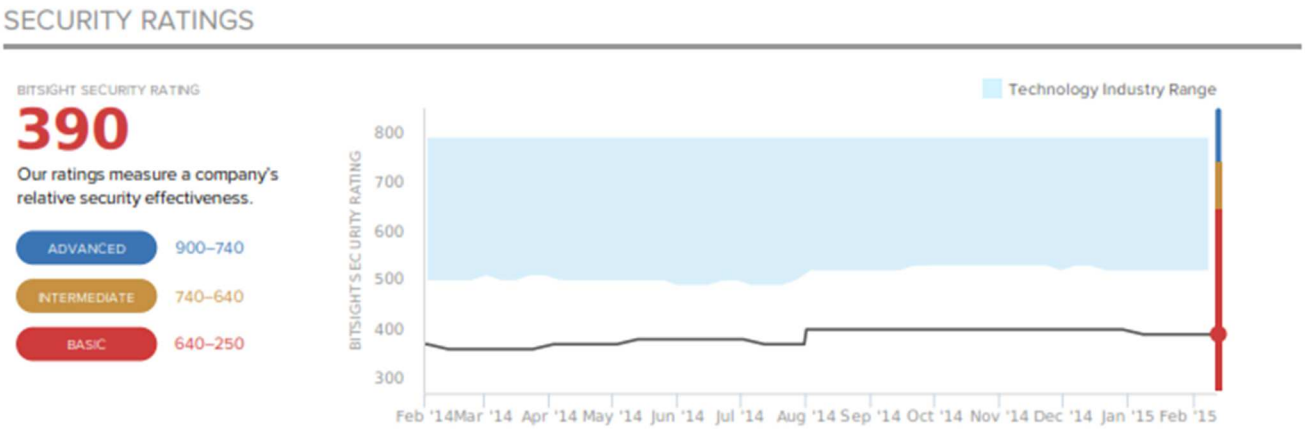
ACCADIMENTO

Sono gli eventi gravi di perdita di dati, ad esempio resi pubblici da varie fonti di notizie, o di hacking condotto con successo. La loro influenza sul Rating è funzione del numero di record "persi" e della loro criticità/sensibilità.

3 e. Perdita di dati accidentale o a seguito di un attacco informatico.
3 f. Azione di attacco informatico condotta positivamente da outsider o da insider.
3 g. Indisponibilità del servizio o del sito web a seguito di attacchi informatici.

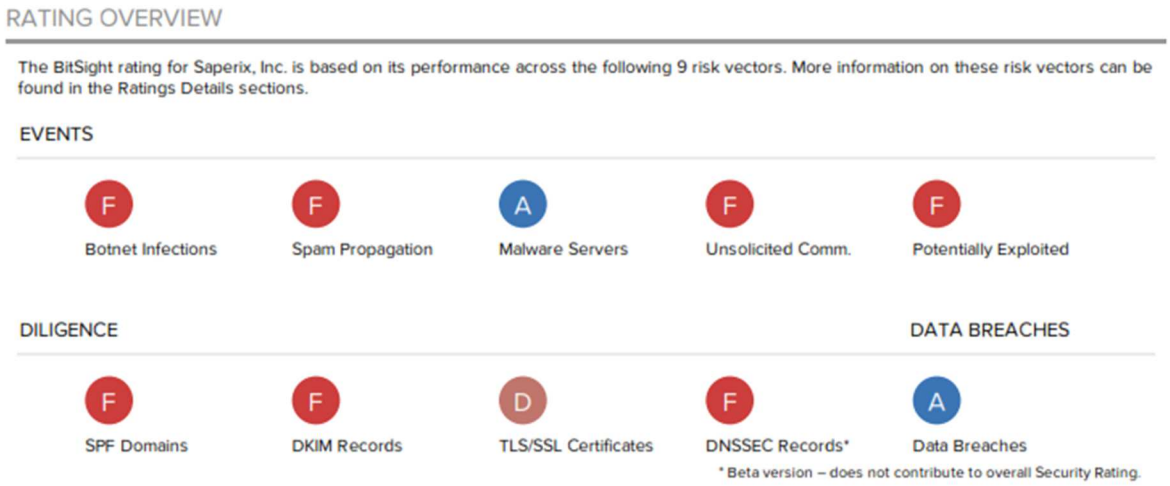
SECURITY RATING – IL SERVIZIO

Il rating calcolato da Xecurity è compreso fra 250 e 900. Insieme al Rating puntuale viene presentato un andamento storico dello stesso ed un grafico che evidenzia il punteggio in questione paragonato alla media delle aziende del medesimo segmento verticale, ad esempio:



La striscia continua azzurra misura la media storica del segmento di industry in questione (qui Technology Industry). La linea continua scura, il rating dell'azienda in esame, non particolarmente favorevole in questo caso!

Viene anche fornito un quadro complessivo dei vari eventi, espresso con un giudizio da A (migliore) a F (peggiore):



DESCRIZIONE DEL SERVIZIO

Il cliente che aderisce al servizio Security Rating di Xecurity è in grado in qualsiasi momento di:

- MONITORARE lo stato della propria sicurezza,
- ANALIZZARE il proprio livello di rischio,
- VERIFICARE la sicurezza di un nuovo fornitore o di un nuovo partner,
- MISURARE lo scostamento rispetto alla sicurezza media del proprio settore di riferimento.

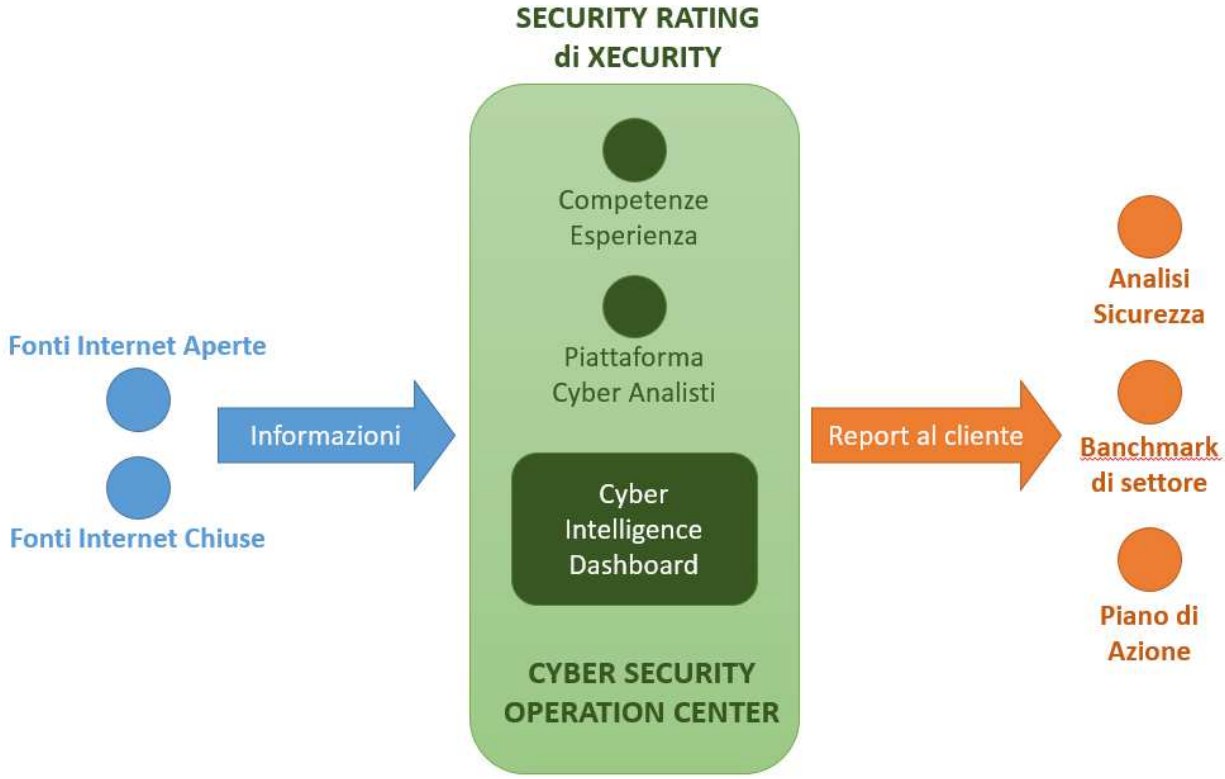
ATTIVAZIONE DEL SERVIZIO

Cominciare a beneficiare delle informazioni è pressoché immediato: basta fornire la ragione sociale e gli indirizzi IP pubblici assegnati dal provider internet.

Dopo qualche giorno si potranno già visualizzare tutte le informazioni sopra dettagliate con i relativi andamenti a partire dall'anno precedente. Xecurity potrà pertanto fornire il primo report con l'analisi di un anno solare.

A seconda del tipo di servizio acquistato la reportistica potrà essere mensile o trimestrale e questo significa che il cliente riceverà ogni mese o ogni trimestre:

- un report che descrive la sua sicurezza, il suo rischio e il suo posizionamento di mercato,
- un sintetico documento contenente le principali fonti di rischio riscontate con la relativa contromisura che si consiglia di adottare.



OPZIONE INTERVENTO

Se poi il cliente decidesse di acquistare anche il supporto on-site, un consulente Xecurity di elevato skill ed esperienza potrà incontrare periodicamente il personale IT per approfondire la lettura dei report ed effettuare insieme le azioni tecniche di contrasto e di rimozione delle minacce riscontrate.

OPZIONE TERZA PARTE

Qualora il cliente necessitasse di avere una fotografia chiara della sicurezza di una terza parte di cui decide di fidarsi, potrà acquistare il relativo servizio di monitoraggio. Essendo un'entità esterna non si avranno (ovviamente) informazioni sulla sua rete interna ma si potrà misurare costantemente il suo livello di sicurezza.