[1]Vicenza, 10/04/2017

TUTTI I RISCHI CYBER – STRATEGIA E TUTELA

Appare ormai inarrestabile la “pacifica invasione” delle tecnologie informatiche in ogni aspetto della nostra vita quotidiana. Innumerevoli i vantaggi, anche se qualche doverosa riflessione occorre farla riguardo al cosidetto “cyber risk”, perche' le entusiasmanti potenzialita' che le tecnologie offrono, possono essere usate anche da hackers e malintenzionati.
Se n'e' parlato a Vicenza nel corso di un convegno promosso da APINDUSTRIA che si e' svolto il 30/03/2017.

I relatori di Italica Forensis hanno sottolineato con attenzione e dovizia di particolari alcune criticita' sollevate dal cybercrime, prospettando da una parte scenari certo non da “sonni tranquilli” ma anche sottolineando quanto sia possibile irrobustire le aziende sul fronte del cyber-risk.

Tra le varie, e' stato ribadito il fatto che gli hackers necessitano di **sistemi effratti** (cioe' aziende intruse a loro insaputa) da utilizzare come **avamposto** da cui sferrare gli attacchi alle loro vittime finali senza operare dalle proprie infrastrutture e rischiare di essere scoperti!

Da questo fatto, la non ovvia considerazione che la sicurezza informatica aziendale non ha solo il compito di **difendere i propri confini aziendali** dagli attacchi effettuati contro di lei, ma anche quello di evitare che la propria infrastruttura sia utilizzata per **attacchi a terzi**.
Situazione che dal punto di vista legale vede l'azienda “**ospite inconsapevole**” correre seri rischi di vedersi chiamata a rispondere **legalmente** dei misfatti compiuti dall'hacker per suo tramite, con un coinvolgimento giudiziario che si puo' ora definire concettualmente: “insufficiente tutela dei livelli di sicurezza interni”.

Altro concetto su cui manca una attenzione adeguata e' il fatto che la commistione tra sistemi **personali** (facilmente insicuri) e sistemi **aziendali** (a sicurezza migliore) e' tale da comportare seri problemi nel momento in cui gli insicuri sistemi personali (portatili, tablet, smartphones) vengono introdotti nelle (fino a quel momento) “sicure” reti aziendali aggirando le difese del firewall ed operando “dall'interno” senza alcun controllo. Oltre naturalmente a quando questi sistemi personali vengono comunque messi a contatto con l'infrastruttura aziendale magari con connessioni remote o trattando dati che poi vengono scaricati in azienda con rischi non indifferenti.

Ulteriore aspetto critico rappresentato al convegno e' quello costituito dallo sfruttamento delle tecnologie wireless da parte degli hackers per **aggirare** le tradizionali difese perimetrali, per **analizzare** ed **aggredire** le reti aziendali senza passare per il firewall ed operando “dall'interno” tramite prospezioni svolte dall'hacker di turno da un bar nei pressi dell'azienda, oppure operando a distanza con intrusioni apposite o con infezioni capaci
di operare come “unita' satelliti” dell'hacker, tutte modalita' ormai “usuali” da parte degli hackers.

Ovviamente si e' parlato dei fenomeni piu' frequenti, quindi anche dei famigerati **cryptolocker** (software che “sequestra” i dati convertendoli in un formato inutilizzabile da cui pagando si puo' riottenere i files originali!) e un cenno e' stato dato anche alle **fatture “ritoccate”** con iban diversi dagli originali (e soldi che i clienti versano convinti che arrivino nel nostro conto originale ma che finiscono altrove!), oltre al tema del **furto di identita'**, particolarmente rilevante, grave e frequente.

Sul fronte del “cosa fare per” non poteva mancare l'aspetto **assicurativo** del “cyber risk”, con polizze ormai massivamente presenti all'estero con un corollario di servizi (tra cui anche un help desk per affrontare l'emergenza). L'Italia su questo fronte e' indietro, le polizze di questo tipo sono ancora in fase di avviamento, anche a causa di una certa reticenza italiana verso gli standard di sicurezza, col risultato che molte aziende non rientrano ancora nei “**minimi sindacali**” di **salute informatica** e di organizzazione sul fronte del rischio industriale. E le assicurazioni vogliono garanzie adeguate prima di assicurare un rischio del genere.

Sul fronte legale ha notevolmente impressionato l'evoluzione sul **fronte normativo**, che ha sostanzialmente operato per una consistente **responsabilizzazione** delle aziende rispetto ai rischi informatici, anche introducendo **responsabilita' civili e penali** in forme finora mai viste. Ciò soprattutto sotto due distinti profili.

Da una parte i **reati informatici** fanno parte dei reati presupposti richiamati dal D.Lgs. n. 231/2001 sulla **responsabilità amministrativa** di Enti e imprese (così definita ma in realtà molto affine, sotto vari profili, a quella **penale**), sicché il loro compimento può comportare responsabilità aggiuntive rispetto a quelle del singolo autore del reato.
Per il caso in cui siano poste in essere alcune condotte tipiche dei reati informatici la legge arriva a prevedere come sanzione per l'Ente o per l'impresa anche l'**interdizione** dall'esercizio dell'attività, misura punitiva che, come si può intuire immediatamente, avrebbe **conseguenze rovinose** sulla persona giuridica responsabile.
Da tenere nel dovuto conto che a parte lo Stato, gli enti pubblici territoriali (Comuni e Regioni), gli altri enti pubblici non economici e gli enti che svolgono funzioni di rilievo costituzionale, il D.Lgs. n. 231/2001 **si applica anche a tutti gli altri Enti Pubblici**.

In secondo luogo il Regolamento UE 679/2016, destinato a sostituire la normativa in materia di privacy fino ad oggi applicata, introduce una serie di **prescrizioni** riferite alle dotazioni informatiche da adottare per difendere Enti e/o Aziende dai **rischi di intrusione**.
Soluzioni informatiche che garantiscono il disaster recovery o che quantomeno siano in grado di **monitorare**, passo per passo e costantemente nel tempo, ogni evento occorso ai sistemi informatici appaiono assolutamente indicati per la **prevenzione** di eventi gravi come la perdita di dati o il danneggiamento irreparabile dei sistemi informatici.
In questi casi l'**apparato sanzionatorio** è d'impatto consistente, perché le violazioni riscontrate dalle autorità garanti possono essere punite con l'irrogazione di pene pecuniarie a partire da varie **decine** di migliaia di euro fino ai **20 milioni** di euro! Per le aziende "top" (ad esempio le grandi multinazionali dell'informatica) si possono applicare sanzioni fino al 4% del fatturato annuale generato a livello mondiale....

Del convegno ha favorevolmente colpito l'approccio ampio ed articolato offerto sull'argomento dai relatori, che hanno trattato in modo **coerente** e **convergente** i fronti "**tecnologico**", "**assicurativo**" e "**legale**", ognuno dei quali ha messo in campo elementi di **prevenzione**, di **analisi** ed anche di **intervento** operativo.

La sintesi e' la seguente: data la grande articolazione delle possibili criticita' di sicurezza esistenti nei sistemi aziendali (e ampiamente sfruttabili dagli hackers), al di la' dei danni che un hacker puo' produrre direttamente, oggi le aziende dovranno mettere in campo impegni consistenti sul fronte della sicurezza informatica anche per evitare pesanti responsabilita' legali, in modo da evitare danni "indiretti" difficilmente calcolabili a fronte di incidenti di sicurezza.

CYBER RISK E PROTEZIONE CIVILE

Tra gli esempi di incidente informatico, gli esperti di Italica Forensis hanno accennato come alcuni di questi possano portare al blocco di **servizi strutturali**, anche di **pubblico interesse**. E qui la Protezione Civile si trova direttamente coinvolta nel tema.

Sono tanti gli esempi: un hacker che blocca una tratta importante dei **servizi elettrici**, potrebbe ad esempio aprire una situazione tipicamente di pertinenza della Protezione Civile.

Analogamente eventi bloccanti massivi riguardanti strutture **bancarie**, servizi **telefonici**, mezzi di **trasporto** (treni, aerei) o strutture industriali dal potenziale rilevante **impatto** sulla collettivita' in termini di servizi erogati (o di impatto a fronte della perdita di controllo tecnologico, pensiamo alle

strutture di controllo di un **bacino** idrico, di un **depuratore**, di una **centrale** termica, di un sistema di distribuzione o di raccolta, etc)... tutto cio' ha come soggetto tipicamente deputato alla gestione delle criticita' connesse o conseguenti l'ente Protezione Civile, in modo assolutamente analogo alle attivita' che l'ente effettuerebbe a fronte di un evento naturale o artificiale "**fisico**" (terremoti, inondazioni, etc).

Questa relativamente nuova "acquisizione" di compiti ed ambiti da parte della Protezione Civile, comporta anche l'acquisizione di know-how specifico, di tecnologie e di metodologie per poter affrontare dal punto di vista **analitico**, **predittivo** e di **pronto intervento** eventi di impatto sociale consistente, oltre naturalmente a permettere all'Ente di tenere prima di tutto in sicurezza la propria infrastruttura tecnologica operativa, sicuramente molto interessante per l'hacker.

Desta una certa impressione il poter (e dover) paragonare l'impatto di specifici eventi informatici alla stregua di un terremoto o di una frana ma, sappiamo: le tecnologie ci sottopongono ormai quotidianamente cose "inconcepibili" fino a ieri, che oggi diventano "cosa normale".

Carloalberto Sartor
Security Engineer

(Pubblicato su LaProtezioneCivile, maggio 2017)