Claudio Bonechi (clavicordo)

ICT CYBERSECURITY FORUM

6 November 2017

Si è svolta a Roma il 25 ottobre 2017 la 18a edizione del Forum **"ICT Security e Business Continuity - dal risk management al crisis management"** presso l'Auditorium della Tecnica, il centro congressi di Confindustria nel quartiere EUR di Roma. Tra gli sponsor e gli intervenuti: Accenture, Vodafone, Boolebox, Hitachi, Symantec, Comitato Atlantico Italiano, Terna, Eni, Snam, Generali, Telecom Italia.

Eccomi quindi nella veste di reporter a darvi un piccolo resoconto di quanto è stato detto in quella occasione.

Intanto, come mia abitudine, renderò esplicite le sigle e le espressioni in inglese che incontriamo; senza offesa per quelli che le conoscono già.

ICT = Information and Communication Technology, che da noi si chiama telematica, mentre IT = Information Technology, è la nostra informatica.

Business Continuity = continuità dei servizi offerti, ossia riduzione al minimo - o, dove possibile, eliminazione – delle interruzioni di servizio. A tutto ciò fanno capo il Backup dei dati continuo, il Disater Recovery (Recupero dati dopo un disatro fisico, quale un terremoto), il Piano di recupero.

Risk management = gestione delle problematiche dei rischi che il sistema informatico corre, in funzione delle proprie vulnerabilità.

IOT = Internet of Things (Internet applicato agli oggetti materiali): è già in atto ma si sta sviluppando in modo esponenziale.

Con **Security** si intende quell'insieme di tecnologie e pratiche finalizzate a proteggere i sistemi informatici e le informazioni in essi memorizzate. In realtà la protezione viene estesa anche alle altre forme di memoria, come i documenti cartacei, e agli aspetti fisici e di comportamento: a tale scopo vengono stabilite delle regole di comportamento, dette "**policy**".

Quando la sicurezza è circoscritta all'ambiente informatico si parla di **Cybersecurity**. E' stato rispolverato quindi il termine *cyber* che deriva da *cibernetica* (cybernetics), coniato da Norbert Wiener nel 1947 e derivato dal greco kybernētik? (tékhnē) = 'arte di guidare, di pilotare'. Il riferimento è alla tecnica del *feedback*, largamente usata dagli organismi biologici, ma in particolare dal timoniere che continuamente corregge la rotta sulla base di riferimenti esterni, che provengono dalla bussola o dalla vista di oggetti del paesaggio. In effetti la cibernetica è la "*scienza che studia i principi di funzionamento e la realizzazione di macchine automatiche, generalmente elettroniche, in grado di simulare le funzioni di organismi viventi e, in particolare, del cervello umano*"; l'emergere dall'intelligenza artificiale ha indotto a formulare negli anni '80 il concetto di "cyberspace" e da qualche anno è nata la cybersecurity.

L'evento conteneva anche vari stand espositivi e, oltre a una forma di pubblicità per gli espositori partecipanti che lo hanno sponsorizzato, è stato anche un **momento di confronto e di aggiornamento** su queste tematiche, caratterizzate da molteplici aspetti, spesso assai complessi. Molti degli espositori hanno presentato i loro prodotti, indirizzati ciascuno a un aspetto diverso.

Riporto di seguito quanto si legge nella **presentazione dell'evento**, con qualche mia libera aggiunta e risistemazione.

"In un contesto macroeconomico in cui la vulnerabilità degli Stati e delle Imprese aumenta, il Risk Management , a garanzia della Business Continuity, è sempre più al centro dell'attenzione di molti amministratori e dirigenti che si interrogano sulle modalità di individuazione, misurazione e trattamento dei rischi in ottica di sicurezza informatica.

Le **funzioni** del Risk Management e della Business Continuity sono:

- proteggere e incrementare il **valore** di un'azienda o di una organizzazione, contribuendo:

· ad un **utilizzo** ed una **allocazione** più efficace del **capitale** e delle **risorse**,

· alla **protezione** del **patrimonio**, dell'**immagine** e del **Know How** (= competenze tecniche, ossia "insieme di conoscenze tecniche necessarie al corretto utilizzo di tecnologie, macchinari, impianti industriali ecc."),

- valutare il potenziale **impatto delle diverse tipologie di rischio** a seconda dei processi, delle attività, dei servizi o dei prodotti, ottimizzando così l'**efficienza operativa** e la **corporate strategy** (= strategia d'impresa).

Minacce in crescita

Le minacce ICT sono in **forte crescita** e colpiscono indifferentemente società di servizi e di consulenza, studi professionali, PMI (Piccole e Medie Imprese), GDO (Grande Distribuzione Organizzata), aziende tecnologiche, marchi di lusso, utilities, infrastrutture critiche ed industrie di ogni settore.

A fronte della **velocità dell'evoluzione delle suddette minacce**, è necessario affiancare ai tradizionali metodi di valutazione del rischio, una aggiornata conoscenza delle proprie vulnerabilità ed una profonda comprensione delle motivazioni, delle capacità e degli strumenti avversari, tramite tecniche avanzate e processi sistematici di **Threat Risk Modeling** (Modellazione del Rischio di Minaccia) e di **Cyber Intelligence** (Intelligenza artificiale applicata ai sistemi informatici)."

Quindi, non solo le **minacce** sono in crescita in senso quantitativo, ma queste minacce si vanno evolvendo, diventano più sofisticate, più **difficili da individuare.**

"Le principali analisi evidenziano con chiarezza quanto la pubblica amministrazione italiana e gran parte del settore industriale siano tuttora fortemente immaturi rispetto alle tematiche che ruotano intorno al mondo della cybersecurity.

Non è un caso, infatti, che l'**Unione Europea** abbia individuato proprio nella resilienza uno dei tre pilastri strategici portanti della sua nuova strategia per la sicurezza cibernetica, così come la **Direttiva NIS** e il Regolamento europeo sulla protezione dei dati (**GDPR**) spingano i principali attori nazionali ad uno sforzo di precisa consapevolezza nei confronti del rischio informatico e della scelta delle più adeguate misure di sicurezza.

Tuttavia, lo scenario attuale e ancor più quello del prossimo futuro - legato soprattutto alla pervasività dell'**Internet of Things (IOT)** per l'ottimizzazione dei processi aziendali - dipingono un quadro in cui mitigare e gestire il rischio informatico **non** sarà più **sufficiente**".

Un problema serio

Insomma, il problema non è solo qualche virus che gira, per il quale basta un buon antivirus. Il problema è serio. Riguarda in primis le grandi organizzazioni, pubbliche e private, ma, più o meno direttamente riguarda **tutti** noi**.** Non c'è bisogno di ricordare che l'informatica permea ogni attività e lo farà sempre di più.

Il **crimine informatico**, fino a non molto tempo fa relativamente limitato, ha assunto **proporzioni preoccupanti**. E' infatti diventato un business allettante, non troppo difficile da attuare, pulito, difficile da contrastare. Viene valutato che il mercatodel cyber-crime mondiale si aggiri intorno ai **400 miliardi di dollari**.

Di seguito ho riportato estratti di presentazioni di espositori, senza citarne il nome.

"Il trend del cyber-crime è in crescita dal 2011 e, secondo il rapporto Clusit (Associazione italiana per la sicurezza informatica), i **danni** provocati in **Italia** dagli attacchi informatici ammontano a **9 miliardi di euro all'anno**."

"Gli attacchi informatici hanno un impatto finanziario sempre più significativo per le organizzazioni di tutto il mondo. Secondo il report "*Cost of Cyber Crime Study*", pubblicato da Accenture e dal Ponemon Institute, che ha coinvolto 2.182 professionisti informatici ed esperti di sicurezza in 254 aziende in tutto il mondo, dal 2009 il numero degli attacchi informatici non ha mostrato segni di rallentamento.

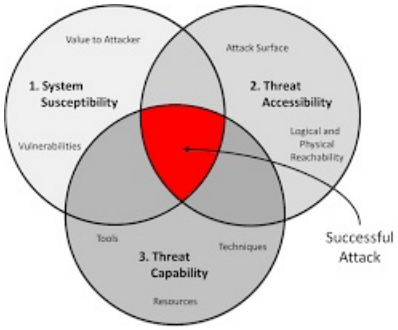
Parallelamente è aumentato anche il **costo medio dei crimini informatici**; questo rapido incremento è il risultato della recente serie di attacchi malware tristemente famosi, come WannaCry e Petya, che a diverse aziende globali sono costati centinaia di milioni di dollari in mancati ricavi.

Il nostro studio mostra inoltre come le allocazioni di spesa in tecnologie di sicurezza siano poco efficaci e si concentrino spesso verso aspetti di pura compliance (=adesioni a requisiti), che non sono però sufficienti. Per fare la vera differenza serve investire in innovazione, guardando alle **nuove tecnologie disponibili,** in particolare agli analytics, all'intelligence e all'intelligenza artificiale e consentono di lavorare in maniera predittiva e non più reattiva."

Gli *analytics* sono "la scienza dell'analisi", ovvero l'applicazione dell'informatica a problemi che richiedono l'analisi e l'interpretazione di un gran numero di dati (Big Data), con lo scopo di stabilire quali siano le migliori decisioni strategiche da prendersi, ad esempio per ottimizzare il business di un'azienda.Solitamente l'analisi viene condotta con metodi statistici con l'applicazione di modelli complessi che effettuano complessi confronti incrociati tra dati anche molto diversi tra loro.

L'"*intelligence*" citata sottintende "business": La *business intelligence* è un concetto a più facce, che comprende processi aziendali, tecnologia per il supporto alla strategia e alle decisioni e tecnologia per la manipolazione ed elaborazione di grosse quantità di dati con fini disparati.

Ossia, dice lui, non basta più affrontare il rischio con i soliti mezzi, “reagendo” alle situazioni critiche. Bisogna cercare di **prevenire il danno probabile**.



Un suggerimento può essere questo: “il 'machine learning' e la matematica stanno automatizzando la rilevazione delle minacce avanzate, attraverso le labili linee di confine della rete; perché la tecnologia self-learning, conosciuta come approccio "immune system", rileva le minacce, non appena cominciano a manifestarsi, senza l'uso di regole e firme; come ottenere il 100% di visibilità della rete in ambienti fisici, IoT, virtuali e Cloud, compresi i servizi Cloud e SaaS (Software As A Service) forniti da terze parti.”

“Oggi è maggiormente importante e rilevante intercettare le *minacce ancora sconosciute*, piuttosto che identificare quelle già note. Circa **30mila nuove varianti di ransomware ogni anno, decine di nuove campagne di phishing ogni giorno**: il canale di diffusione principale è l’**e-mail**. Alimentato e motivato da un giro d'affari di centinaia di milioni di euro, il business del malware evolve continuamente.”

“L’ultimo **Rapporto Clusit** evidenzia che nel 2016 gli attacchi informatici hanno creato danni per un valore complessivo stimato di 30 miliardi di euro, colpendo in particolare alcuni settori: si va dalla Sanità (+102% di attacchi rispetto all’anno precedente) al Finance (+64%), fino al mondo delle Infrastrutture Critiche (+15%).”

Come è per altri argomenti informatici, anche la cybersecurity è oggetto dei sistemi di qualità, nel senso che per raggiungere certi livelli di protezione deve soddisfare un certo numero di **requisiti**. Questi requisiti sono stati elaborati e raccolti in alcuni standard internazionali come il **Nist** e le **ISO 27001**.

Assicurazione

"Le migliori pratiche di gestione del rischio motivano l'interesse di aziende di ogni dimensione e settore merceologico verso nuove **soluzioni assicurative** in grado di trasferire il rischio informatico" (università di Modena).

Tutti sono d'accordo che un'assicurazione è **necessaria** ma non è una cosa semplice ottenere una polizza assicurativa che copra i danni da attacchi informatici. L'assicuratore ha a che fare con

una situazione assai scivolosa, soprattutto a causa della continua evoluzione delle minacce: questo impedisce la costruzione dell'equivalente delle tabelle attuariali.

Le Compagnie assicurative, quindi, non possono fare altro che una scommessa sul rischio da assicurare, quindi correre un rischio a loro volta. Ne segue che solo quelle grandi possono permettersi questo rischio; quelle piccole stanno a guardare cosa succede. Ciononostante in USA la stipula di polizze assicurative è in **aumento del 35% annuo**.

Il GDPR

L'Europa ha partorito un Regolamento Generale per la Protezione dei Dati o **General Data Protection Regulation (GDPR)**, già in vigore dal 4 Maggio 2016, che diventerà **efficace il 25 Maggio 2018** e che impone l'adesione (compliance) a una serie di norme. "Il regime di protezione dei dati proposto per l'UE estende gli obiettivi della legge europea sulla protezione dei dati a tutte le imprese estere che trattano dati di residenti europei a prescindere dal luogo nel quale le trattano e dalla loro sede legale. Permette di armonizzare le diverse normative sulla protezione dei dati in tutta l'UE, facilitando così l'osservanza delle norme da parte delle imprese non europee; tuttavia, questo è stato ottenuto a costo di un regime di una severa disciplina di protezione dei dati, con rigide sanzioni che possono raggiungere i 20.000 Euro o il 4% del volume globale di affari."

Ecco, notiamo bene questo punto: a differenza della precedente legge sulla privacy 196 del 2003, che non le prevedeva sanzioni, il GDPR prevede **sanzioni**, eccome! So per certo che il Garante sta organizzando una task force di controllo che, a quanto si dice in giro, non farà sconti a nessuno. Anche se molti pensano che tutto finirà all'italiana. Ma non è detto. Staremo a vedere.

Un punto importante del GDPR è l'**obbligo per le organizzazioni** di segnalare all'autorità designata certi tipi di "**data breach**", cioè quegli attacchi riusciti al sistema informatico che portano alla distruzione, perdita, alterazione, accesso non autorizzato, rivelazione di dati critici per la libertà degli individui. Riporto il glossario del Garante della privacy:

"**Dato personale**

Qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo.Sono, ad esempio, dati personali: il nome e cognome o denominazione; il'ndirizzo, il codice fiscale; ma anche un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc..

Dato sensibile

Un dato personale che, per la sua natura, richiede particolari cautele: sono dati sensibili quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Dato giudiziario

I dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).

Rientrano in questa categoria anche la qualità di imputato o di indagato.

I soggetti che procedono al trattamento dei dati personali altrui **devono** adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati." (dal sito garanteprivacy.it)

Gestione del rischio informatico

"La **gestione del rischio informatico e la conseguente gestione della crisi**, immediatamente successiva ad un attacco andato a segno, sono divenuti ormai dei nodi fondamentali al fine di proteggere le Organizzazioni da ingenti danni economici e di immagine. Con il GDPR viene introdotto il principio di **responsabilizzazione (accountability)** che richiede da parte di titolari e responsabili del trattamento un approccio diverso, attivo in tutte le fasi del trattamento a cominciare dalla privacy *by design* e *by default*. Questi sono solo alcuni dei punti con i quali le Supervisory Authority, i titolari e i responsabili del trattamento devono lavorare affinché siano operativi **prima della data del 25 maggio prossimo .**

Phishing! State attenti!

Un'altra problematica emersa è quella del **Phishing**, che consiste in una "**truffa informatica** effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico".

Per quanto il Phishing sia conosciuto e le truffe informatiche frequenti, è tuttavia un'arma molto efficace in mano ai criminali, perché non è sempre facile capire che il messaggio email è ingannevole. Durante la presentazione sono stati mostrati dei casi in cui era praticamente impossibile accorgersene. Come contromisura, esistono dei programmi che producono Phishing, allo scopo di esercitare il personale di un'organizzazione a riconoscere l'inganno.

Ciò mi induce a evidenziare un punto importante tra quelli trattati e cioè la **formazione del personale**. Molti danni informatici (circa il 60%) provengono da comportamenti inadeguati delle persone interne all'organizzazione, sia per dolo, sia per trascuratezza (ad esempio usare password banali, non cambiarle spesso), sia per ignoranza. La formazione in campo Cybersecurity è in effetti considerata da tutti un elemento fondamentale della **prevenzione**.

Un punto evidenziato particolarmente nella tavola rotonda è la collborazione e lo scambio immediato di informazioni tra organizzazioni che hanno subìto attacchi o che li hanno individuati come potenziali. Il fattore tempo è infatti essenziale e quindi più rapidamente si viene a conoscenza degli accadimenti dannosi e più è probabile intervenire e rimediare con successo, limitando le perdite.

Conclusione

Ho cercato di fare, con questo riassunto della giornata ICT Security Forum, di presentare una panoramica di argomenti sulla sicurezza informatica, che in realtà è un campo di attività molto vasto e complesso, che implica investimenti impegnativi. Ma ormai le dimensioni del cyber-crime sono tali che nessuno di noi, sia a livello di organizzazioni lavorative che a livello familiare e individuale può permettersi di ignorarlo.

Per inciso, ricorderò anche che il crimine non è il solo aspetto malevolo associato al cyberspazio. Ce n'è un altro molto più inquietante ed è il **CyberWar**, ossia la guerra informatica il cui attore protagonista principale sembra essere il terrorismo. Ma certamente non è il solo: ne abbiamo un esempio recente con il Russiagate, di cui non sappiamo praticamente nulla e meno ancora sappiamo di tanti altri fatti simili.

Inoltre è facile pensare che **le "armi" informatiche tendono a sostituire le armi tradizionali**, perché in prospettiva, con lo IOT, possono produrre danni incalcolabili al nemico, a costi decisamente più bassi. Con conseguenze inimmaginabili sull'economia generale.

Un'ultima notazione. **La Cybersecurity è un business in forte crescita**; lo si vede anche dal numero dei convegni e degli eventi. Ciò apre lo spazio a **nuove professionalità**. I giovani dovrebbero tenerne conto seriamente.

Estratto da "http://www.electroyou.it/mediawiki/index.php?title=UsersPages:Clavicordo:ict-cybersecurity-forum"