Cyber security: dalle tecnologie alle procedure organizzative

Aziende di servizi, banche, imprese manifatturiere e distributori di tecnologie e soluzioni software a confronto sulla sicurezza. Tra consapevolezza e best practice, ecco come le PMI si difendono

di Veronica Pastaro

Assistiamo ormai a un continuo aumento di attacchi cyber che diventano sempre più complessi e articolati e avvengono sfruttando una combinazione di vulnerabilità umane e tecnologiche che permettono ai cyber criminali l'ingresso all'interno dell'organizzazione. I dati dell'ultimo rapporto CLUSIT (l'Associazione italiana per la sicurezza informatica) sono allarmanti: nel 2015 il cyber crime è cresciuto di circa il 30%, lo spionaggio di quasi il 40%, gli attacchi alle strutture critiche del 150%; le perdite economiche sono aumentate di quattro volte dal 2013, determinando un danno pari a quasi un punto di PIL. In particolare l'Italia si colloca al decimo posto nella classifica dei Paesi più colpiti, ma al tempo stesso evidenzia un incremento di investimenti del 5% in sicurezza.
L'obiettivo di simili attacchi non è rappresentato soltanto da banche e grandi multinazionali: gran parte del fatturato di queste azioni criminali è infatti realizzato colpendo decine di migliaia di medie, piccole e micro imprese completamente impreparate ad affrontare efficacemente la minaccia.
I criminali bloccano l'operatività di queste imprese per poi chiedere un riscatto, rubano i loro asset, i dati o spiano le strategie di business, al punto da mettere a rischio la sopravvivenza stessa dell'organizzazione. Tuttavia molti di questi attacchi sfruttano vulnerabilità 'banali' presenti nei sistemi informativi dell'azienda o una mancanza di consapevolezza della problematica da parte del personale interno, come ben illustra Andrea Rossetti, Professore Associato di Filosofia del diritto e di Informatica giuridica dell'Università di Milano Bicocca, nel suo articolo *Il fattore umano nella sicurezza: Educare alle percezione del rischio* (qui a pp. 44-49).
L'innalzamento dei livelli di security delle piccole e micro imprese è un passaggio fondamentale per la messa in sicurezza delle filiere produttive, dal momento che un numero sempre maggiore di attacchi a grandi imprese capo-filiera viene infatti realizzato grazie a vulnerabilità presenti nelle aziende che compongono le loro filiere.
Il crescere delle pratiche in materia di cyber security risulta particolarmente importante in un

Un momento della tavola rotonda 'Servizi, banche e pharma'


Gennaro Auriemma, Wind Tre


Carlo Brezigia, Intesa San Paolo Group Services


Massimiliano Grassi, Citrix


Riccardo Riccobene, Deutsche Bank Italia

momento di forte trasformazione digitale del settore industriale che aumenterà l'integrazione tra le aziende appartenenti a una filiera, rendendo ancor più estesa, di conseguenza, anche la superficie d'attacco. *Sistemi&Impresa* ha organizzato due tavole rotonde con i rappresentanti di 11 aziende che si sono confrontati sul tema della sicurezza dei dati in Italia, sul livello di conoscenza delle imprese e su possibili best practice da implementare nel prossimo futuro.

Strutture a sostegno della sicurezza

La repentina trasformazione del contesto di riferimento porta con sé la necessità di intervenire con modifiche strutturali all'interno delle stesse organizzazioni, talvolta con la creazione di nuovi processi *ad hoc*. È il caso di Wind Tre, azienda guidata da Maximo Ibarra, nata dalla fusione fra H3G e Wind Telecomunicazioni, che ha creato un Security operation center per rilevare attacchi informatici e definito processi trasversali a diverse aree aziendali per gestire eventuali violazioni dei dati personali. Spiega **Gennaro Auriemma, Responsabile Security Engineering di Wind Tre**: "Dopo l'introduzione di provvedimenti in materia di sicurezza, abbiamo adottato una serie di misure e best practice, che anticipano molti adempimenti della direttiva UE che presto sarà in vigore. Come operatore di telefonia fissa e mobile, infatti, siamo molto attenti alla protezione dei dati, sia per quanto riguarda le attività interne sia per i servizi che forniamo ad aziende e PMI".

Parallelamente **Carlo Brezigia, Responsabile Servizio Information Security & Business Continuity di Intesa San Paolo Group Services**, illustra come la protezione informatica entri in gioco già a partire dalla definizione del design: "Prima ancora di valutare il rischio dal punto di vista tecnologico, analizziamo una moltitudine di scenari, ponendo una particolare attenzione a tutta la sfera dei comportamenti degli utenti e dei dipendenti che possono essere indotti dalla struttura stessa delle piattaforme".

Sull'altro fronte, Citrix, società che fornisce tecnologia per rendere il mondo delle app e dei dati sicuro e di facile accesso con ogni device e su ogni Rete, punta su pacchetti altamente personalizzati, proprio sulla base delle necessità dinamiche dei clienti. "A prescindere dal livello di consapevolezza dei rischi, le nostre architetture garantiscono all'IT la concessione di flessibilità verso gli utenti stessi per poterne liberare la produttività al meglio, senza tuttavia bisogno di imporre divieti", spiega **Massimiliano Grassi, Marketing Manager Italy, SouthEastern Europe & Israel di Citrix**.

Descrivono la loro esperienza in materia di attacchi alla sicurezza il gruppo farmaceutico Sanofi e Deutsche Bank Italia, mettendo in evidenza quali fattori rendono sempre più complicate le operazioni di difesa.

"Richiedono di innalzare il livello di allerta soprattutto telefonate o email molto mirate, con specifica di nome e cognome, talvolta persino profilate sulla base di interessi privati, e pertanto capaci di trarre in inganno con molta facilità. Si verificano inoltre richieste di informazioni attinenti ai settori di compe-

I partecipanti alla tavola rotonda: "SERVIZI, BANCHE E PHARMA"

Gennaro Auriemma, Responsabile Security Engineering – **WIND TRE**
Carlo Brezigia, Responsabile Servizio Information Security & Business Continuity – **INTESA SAN PAOLO GROUP SERVICES**
Massimiliano Grassi, Marketing Manager Italy, SouthEastern Europe & Israel – **CITRIX**
Riccardo Raschini, Head of General Affairs & Security – **SANOFI**
Riccardo Riccobene, COO Chief Information Security Office – **DEUTSCHE BANK ITALIA**

Eros Gelfi, Lucchini Mamé Forge

Gianluca Nardin, Carel

Mattia Paolini, Nanosoft

Claudio Panerai, Achab

tenza, che non destano alcun tipo di sospetto", racconta **Riccardo Raschini, Head of General Affairs & Security di Sanofi**.
Ancora più incalzanti e frequenti sono le attività riportate da **Riccardo Riccobene, COO Chief Information Security Office di Deutsche Bank Italia**: "In un contesto bancario come il nostro, che cerca di adattare sempre più la propria interfaccia all'innovazione, registriamo una media di sette attacchi al secondo, che rendono necessario attuare strategie difensive, non soltanto dall'esterno, ma anche dal lato clienti. Per questa ragione risulta prioritario per noi individuare quali sono i comportamenti abituali di questi ultimi, in modo da riscontrare nel più breve tempo possibile eventuali anomalie".
Dall'esperienza delle aziende attorno alla tavola rotonda, relativa al mondo di servizi e banche, emerge come l'attenzione alle tematiche di sicurezza sia strettamente dipendente dalle dimensione dell'azienda e come, pertanto, si possano riscontrare differenti gradi di maturità. Ciononostante è percezione diffusa che il middle management italiano si stia dimostrando altamente recettivo, consapevole che un rischio IT pari a zero è inesistente.

Generare consapevolezza dei rischi

Anche il mondo dell'industria manifatturiera non è esente da attacchi e il come prevenirli rappresenta una domanda sempre più pressante. Lucchini Mamé Forge, azienda che si occupa della produzione di forgiati speciali, ha previsto all'interno del suo codice etico un apposito paragrafo sul tema della sicurezza: "Il primo passo che ci è sembrato fondamentale compiere è stato formalizzare in modo chiaro il divieto di installare software privati sui computer aziendali, considerata la media di 3mila email all'ora, di cui il 98% rappresentato da spam", dice **Eros Gelfi, CTO di Lucchini Mamé Forge**.
Gianluca Nardin, IT Technology Manager di Carel, leader mondiale nelle soluzioni di controllo per condizionamento, refrigerazione e riscaldamento, rileva una scollatura di percezione consistente lato business e lato IT: "Spesso le aspettative business erano disattese perché l'approccio non era olistico, ma si puntava solo su investimenti tecnologici. Abbiamo invece creato un team interfunzionale, anche con lo scopo di aumentare il grado di consapevolezza in materia di sicurezza. Mettendo a fattore comune le esperienze di altre aziende amiche, abbiamo inoltre accelerato l'evoluzione del progetto con un notevole risparmio di tempo ed energie, per esempio nell'identificazione delle soluzioni disponibili sul mercato".
Nanosoft, azienda del gruppo Sme.UP, che propone un percorso di sviluppo nelle tecnologie informatiche a tuttotondo, dall'infrastruttura al middleware, fino ad arrivare al software applicativo, è testimone di una sostanziale incoerenza da parte delle aziende clienti: "Chi è in cerca di una soluzione in materia di sicurezza, vorrebbe risolvere la propria situazione nel più breve tempo possibile, spesso però senza neanche sapere quale sia l'effettivo problema, nonostante sia noto che nella maggior parte dei casi l'attacco viene scoperto con un ritardo considerevole, circa tre-sei mesi dopo", afferma **Mattia Paolini, Sales & Marketing Manager di Nanosoft**. "Purtroppo a tutt'oggi la sicurezza non è vista come un elemento qualitativo del proprio business".
Risulta quindi prioritario investire in formazione: "Oltre a proporre software e soluzioni ICT flessibili, efficaci ed economicamente convenienti, il nostro obiettivo è accompagnare le PMI attraverso un incessante percorso di presa di consapevolezza delle opportunità e dei rischi", illustra **Claudio Panerai, CTO di Achab**. "Secondo noi proteggere il patrimonio significa prima di tutto formarsi e poi investire per essere pronti a reagire".

I partecipanti alla tavola rotonda: "MANIFATTURA"
Eros Gelfi, CTO – **LUCCHINI MAMÉ FORGE**
Gianluca Nardin, IT Technology Manager – **CAREL**
Mattia Paolini, Sales & Marketing Manager – **NANOSOFT**
Claudio Panerai, CTO – **ACHAB**

BEST PRACTICE: 15 'CONTROLLI ESSENZIALI' DI CYBER SECURITY

Il *Cyber Security Report 2016*, realizzato dal Centro di Ricerca CIS dell'Università La Sapienza di Roma, propone *15 Controlli Essenziali* che possono essere adottati e implementati da medie, piccole o micro imprese per ridurre le vulnerabilità presenti nei loro sistemi e per aumentare la consapevolezza del personale interno, in modo da resistere agli attacchi più comuni. Per controllo essenziale si intende una pratica relativa alla cyber security che, qualora ignorata oppure implementata in modo non appropriato, causerebbe un aumento considerevole del rischio informatico. Le pratiche proposte sono di facile e, quasi sempre, economica implementazione e rappresentano una serie di controlli di sicurezza che non possono essere ignorati.

1. Creare e mantenere aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2. Utilizzare soltanto i servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti strettamente necessari.
3. Individuare le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4. Nominare un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5. Identificare e rispettare le leggi e/o i regolamenti con rilevanza in tema di cyber security che risultino applicabili per l'azienda.
6. Dotare tutti i dispositivi che lo consentono di software di protezione (antivirus, antimalware, ecc.) regolarmente aggiornato.
7. Diversificare le password per ogni account, con una complessità adeguata e valutare l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (per esempio autenticazione a due fattori).
8. Mettere il personale autorizzato all'accesso ai servizi informatici, da remoto o da locale, nelle condizioni di disporre di utenze personali non condivise con altri. Proteggere opportunamente l'accesso e disattivare i vecchi account non più utilizzati.
9. Fare in modo che ogni utente possa accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10. Sensibilizzare e formare adeguatamente il personale sui rischi di cyber security e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (per esempio riconoscere allegati email, utilizzare solo software autorizzato, ecc.). I vertici aziendali devono avere cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11. Far svolgere la configurazione iniziale di tutti i sistemi e dispositivi da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default devono essere sempre sostituite.
12. Eseguire periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). Conservare i backup in modo sicuro e verificarli periodicamente.
13. Proteggere le Reti e i sistemi da accessi non autorizzati attraverso strumenti specifici (per esempio Firewall e altri dispositivi/software anti-intrusione).
14. In caso di incidente (per esempio venga rilevato un attacco o un malware), informare i responsabili della sicurezza e far mettere in sicurezza i sistemi da personale esperto.
15. Aggiornare tutti i software in uso (inclusi i firmware) all'ultima versione consigliata dal produttore. Dimettere i dispositivi o i software obsoleti e non più aggiornabili.

I partecipanti alla tavola rotonda 'Manifattura'

Non mancano iniziative fantasiose da parte delle aziende: c'è chi intrattiene giochi di ruolo con malintenzionati al fine di studiarne strategie e comportamenti, scoprendo tuttavia di non disporre del supporto delle autorità per il reato di phishing; e c'è chi avvia vere e proprie simulazioni interne al contesto aziendale, per mappare tempistiche e differenti reazioni. Sono così state clusterizzate due tipologie di modi di agire: da una parte i comportamenti attesi e dall'altra quelli omertosi. Appare perciò evidente l'importanza di educare i dipendenti al rischio affinché comprendano che dichiarare di essere stati vittime di un'azione di phishing è meno dannoso (per sé e per l'azienda) rispetto al nasconderlo; infatti, finché l'attacco non viene rilevato, risulta impossibile per l'organizzazione difendersi e quindi adoperarsi per la risoluzione dei problemi arrecati.