Cybersicurezza. Imprese sempre più digitali ma il malware è causa di incertezza nel business

L'uragano informatico che spaventa le aziende

Costi medi di 5,5 milioni l'anno - Da maggio il regolamento Ue

Biagio Simonetta

Sempre più digitali ma anche sempre più spaventate dal rischio di un cyber attacco. Le aziende italiane, a quanto pare sono uscite dal limbo dell'inconsapevolezza che le avvolgeva fino a qualche tempo fa, e oggi temono veramente la portata di un'intrusione informatica. Secondo uno studio di Allianz (Allianz Risk Barometer) pubblicato ieri, i rischi informatici si posizionano sul secondo gradino del podio fra quelli più temuti dalle imprese italiane in questo 2018. E del resto, basta dare un'occhiata ai numeri diffusi da Accenture per capirsi: in Italia ogni azienda subisce in media un costo di ben 5,5 milioni di euro all'anno a causa di attacchi informatici. Tanti soldi.

«Sottovalutato per molto tempo, il rischio informatico è una preoccupazione crescente per le aziende italiane, e anche il danno reputazionale è una minaccia in aumento» ha detto, Nicola Mancino, ceo di Allianz Global Corporate & Specialty Italia, commentando i numeri diffusi proprio da Allianz che raccontano come per la prima volta nella storia, l'interruzione di attività e il cyber risk hanno la stessa importanza per i manager. Un risultato spinto, molto probabilmente, da eventi che nel corso del 2017 hanno posto grande attenzione sul rischio informatico per le imprese. Un caso su tutti: WannaCry, il malware di tipo ransomware che a maggio scorso ha colpito più di centomila sistemi informatici in tutto il mondo, mandando in tilt centinaia di aziende e decine di ospedali.

WannaCry (ma successivamente anche l'attacco denominato Petya) hanno in qualche modo dato una scossa alla percezione un po' assonnata delle aziende italiane. «Che si tratti di attacchi come WannaCry, o più frequentemente di guasti di sistema, - ha detto Chris Fischer Hirs, ceo di Allianz Global Corporate & Specialty commentando i dati dell'ultimo report - gli incidenti informatici sono oggi una delle principali cause di interruzione di attività per le aziende collegate in rete, i cui principali asset sono spesso i dati, le piattaforme di servizio o i loro gruppi di clienti e fornitori».

Un 2017 da paura

Se il 2016 era stato ribattezzato come anno da incubo dal rapporto Clusit («il peggiore di sempre»), per il 2017 non c'è da aspettarsi nulla di buono. I casi già citati WannaCry e Petya sono solo la punta dell'iceberg di un fenomeno che ha travolto anche le imprese. E vale la pena ricordare qualche caso tutto italiano. A gennaio dello scorso anno, quattro Pmi venete subirono un importante attacco informatico basato su un malware di tipo ransomware che le ha costrette a pagare un riscatto per poter riavere accesso ai loro computer. Come di consueto, i nomi delle quattro aziende colpite non vennero alla galla: il danno reputazionale gioca sempre a favore degli hacker, in casi come questo, con le aziende colpite che preferiscono non uscire allo scoperto. Non potè rimanere nell'anonimato, invece, l'attacco ai danni di Unicredit, che a luglio ha subito un'intrusione pesantissima nei suoi sistemi, con i dati anagrafici, le posizioni e gli Iban di 400mila clienti italiani finiti nel mirino dei criminali informatici.

IL PRECEDENTE

Un caso su tutti: WannaCry, il virus di tipo ransomware che nel maggio scorso ha colpito più di centomila sistemi nel mondo

LA PAROLA CHIAVE

Malware

Con il termine malware si intende l'abbreviazione per malicious software (software dannoso), indicativa di un qualsiasi software utilizzato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati oppure mostrare pubblicità indesiderata. Il termine malware è stato coniato nel 1990, precedentemente veniva chiamato virus per computer; in italiano viene anche comunemente chiamato codice maligno.

L'incognita Gdpr

Di certo possiamo dire che nei prossimi anni, i potenziali "uragani informatici" e le norme più severe in materia di protezione dei dati caratterizzeranno l'ambito del rischio informatico. E fra queste va segnalato senza alcun dubbio l'entrata in vigore del Gdpr, nuovo regolamento europeo sulla protezione dei dati personali che le aziende dovranno recepire entro il 25 maggio 2018. Una data non rinviabile, che nelle sedi di molte imprese italiane suonerà come un gong. Il Gdpr è un regolamento, e i regolamenti non richiedono provvedimenti legislativi da parte degli stati membri. Per chi non applicherà le nuove regole imposte dal garante europeo saranno dolori: le infrazioni saranno sanzionate pesantemente, potendo raggiungere ammende fino a 20 milioni di euro o fino al 4 per cento del fatturato annuale.

A fronte delle sanzioni previste, c'è un costo da sostenere per adeguarsi che non è certo trascurabile. La spesa riguarda nuove consulenze e acquisto nuove tecnologie, e non è un caso che alla voce cyber sicurezza ci sia un forte segno "più" negli investimenti delle imprese italiane.

Secondo una ricerca di Ernst & Young Il valore medio di investimento per l'adeguamento al Gdpr per le aziende, nel 2016 era di 349mila euro, mentre nel 2017 è salito a 480mila. L'investimento complessivo nel 2017 è stato di 6,5 Miliardi di Euro su 30.000 aziende.

Per Gabriele Faggioli, responsabile scientifico dell'Osservatorio Information Security & Privacy del Politecnico di Milano, è molto difficile stimare il costo - in termini assoluti - che le aziende devono sostenere per adeguarsi al nuovo regolamento sulla protezione dei dati. «Direi che innanzitutto è meglio distinguere fra pubblico e privato. - ha detto Faggioli al Sole 24 Ore – E poi nel privato è obbligatorio distinguere grandi aziende da piccole e medie imprese».

Secondo il responsabile dell'Osservatorio milanese, per quanto concerne le grandi aziende (non le big company) «i costi di consulenza per adattarsi al Gdpr sono stimabili in centinaia di migliaia di euro per azienda», mentre per le Pmi i costi possono variare «dai 10mila ai 40mila euro a seconda di fatturato e dimensioni». Sullo stato di fatto, Faggioli non nasconde una certa preoccupazione: «Le nostre stime (che prossimamente finiranno in un nuovo studio, ndr) ci dicono che le grandi aziende sono abbastanza pronte al nuovo regolamento. La pubblica amministrazione, invece, mi lascia molti dubbi». Chiusura sulle Pmi: «Sono quelle più in ritardo».

I rischi più temuti dalle aziende italiane

LA TOP 10 DEI RISCHI IN ITALIA

1 = Interruzione di attività
2 ↑ Rischi informatici
3 = Catastrofi naturali
4 ↑ Danno reputazionale o d'immagine
5 ↑ Incendio, esplosioni
6 ↑ Nuove tecnologie
7 = Cambiamenti legislativi
8 ↓ Cambiamenti nei mercati
9 ↑ Cambiamento climatico
10 ↑ Rischi ambientali (inquinamento)

LA TOP 5 PER SETTORE

Aeronautico

1. Interruzione di attività	45%
2. Rischi informatici	44%
3. Cambiamenti nei mercati	33%
4. Cambiamenti legislativi	26%
5. Rischi politici	26%

Marittimo

1. Catastrofi naturali	34%
2. Interruzione di attività	31%
3. Rischi informatici	31%
4. Furto, frode, corruzione	27%
5. Incendio, esplosioni	25%

Food

1. Interruzione di attività	53%
2. Danno reputazionale	31%
3. Catastrofi naturali	27%
4. Mancanza di qualità	24%
5. Incendio, esplosioni	21%

Tlc

1. Rischi informatici	77%
2. Interruzione di attività	44%
3. Catastrofi naturali	33%
4. Cambiamenti legislativi	28%
5. Danno reputazionale	23%

Manifatturiero

1. Interruzione di attività	74%
2. Rischi informatici	40%
3. Catastrofi naturali	32%
4. Incendio, esplosioni	29%
5. Mancanza di qualità	20%

Oil & Gas

1. Catastrofi naturali	53%
2. Incendio, esplosioni	49%
3. Interruzione di attività	46%
4. Rischi informatici	31%
5. Rischi ambientali	22%

Energia

1. Interruzione di attività	58%
2. Rischi informatici	47%
3. Catastrofi naturali	46%
4. Incendio, esplosioni	29%
5. Cambiamenti legislativi	24%

Trasporti

1. Interruzione di attività	37%
2. Furto, frode, corruzione	32%
3. Rischi informatici	29%
4. Catastrofi naturali	25%
5. Cambiamenti legislativi	24%

Tecnologia

1. Rischi informatici	59%
2. Interruzione di attività	42%
3. Nuove tecnologie	35%
4. Cambiamenti legislativi	25%
5. Cambiamenti nei mercati	19%

Real estate

1. Catastrofi naturali	45%
2. Interruzione di attività	40%
3. Incendio, esplosioni	29%
4. Rischi informatici	22%
5. Cambiamenti nei mercati	21%

Fonte: Allianz Global Corporate & Specialty.