Il cybercrime sale al primo posto tra i timori delle aziende italiane

Il "Regional Risks for Doing Business Report 2019" realizzato dal World Economic Forum (Wef) registra una sempre maggiore importanza dei rischi informatici nella prevenzione e gestione dei rischi d'impresa.

Il rischio cyber, nel 2018, non compariva nemmeno tra i primi cinque rischi percepiti da manager d'azienda e imprenditori europei e italiani. Secondo il ***Regional Risks for Doing Business Report 2019*** del Wef, invece, la proliferazione degli attacchi informatici ha fatto salire il cyber risk al primo posto in Europa e in Italia.

I cyber attack sono ormai così sofisticati e frequenti da richiedere un'attenzione costante alla sicurezza informatica nella gestione dei rischi in azienda.

Il rischio cyber è salito dal quinto posto del 2018 al secondo posto tra i rischi maggiormente percepiti a livello mondiale. Lo rileva il *Regional Risks for Doing Business Report 2019*, che ha coinvolto oltre 13 mila business leader in 130 Paesi nel mondo con lo scopo di classificare le principali paure legate allo svolgimento della loro attività per i prossimi dieci anni.

I rischi collegati alle tecniche di hackeraggio informatico, come il rischio di frodi o furto di dati entrano nella top 5 in Italia, mentre a livello europeo e globale si classificano rispettivamente al sesto e settimo posto.

Top ten business risks of highest concern globally

1. Fiscal crises	6. Profound social instability
2. Cyberattacks	7. Data fraud or theft
3. Unemployment or underemployment	8. Interstate conflict
4. Energy price shock	9. Failure of critical infrastructure
5. Failure of national governance	10. Asset bubble

Gli attacchi a strutture pubbliche e private e la vulnerabilità dei dati personali a disposizione delle aziende hanno fatto aumentare il timore fra manager e imprenditori per quanto riguarda la sicurezza informatica, che è oramai cruciale elemento di prevenzione per la pianificazione e la gestione del business.

Attacchi informatici, furti di dati personali, falle e intrusioni tecnologiche possono infatti intaccare la reputazione di un'azienda. Non solo, la perdita di dati e informazioni possono essere sanzionate secondo quanto previsto dal Regolamento Europeo sui Dati Personali (GDPR).

Per ridurre il rischio cyber è più che mai fondamentale, soprattutto nelle aziende, la formazione e l'assimilazione di una cultura del rischio e della prevenzione.

A questo mira l'ECSM (European Cybersecurity Month), una campagna dell'Unione Europea che dura tutto il mese di ottobre e promuove la conoscenza delle minacce informatiche e dei metodi per contrastarle, per cambiare la loro percezione dei cyber risk e fornire informazioni aggiornate e utili alla protezione cibernetica e sicurezza informatica. L'ECSM è organizzato dall'agenzia europea ENISA e prevede diverse attività in tutti i Paesi membri dell'UE.

In Italia, il Mese Europeo della Sicurezza Informatica è supportato da CLUSIT [ndr: che redige anche il più completo rapporto italiano sui rischi cyber, e scaricabile nell'area Fintech di AITI] e varie organizzazioni, Università e Centri di Ricerca, in accordo con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Conoscere ed essere consapevoli dei diversi tipi di minacce legate al **sistema informatico aziendale** è il primo passo per tutelare il frutto del proprio lavoro, dati e risorse economiche. Di seguito potete trovare alcune delle principali attività cyber criminali e di capire qual è il riferimento normativo di ciascuna di esse.

Hacking

- **Accesso abusivo ad un sistema informatico o telematico**: questo reato vede una persona ottenere l'accesso ad un sistema informativo protetto contro il consenso esplicito o implicito della persona avente diritto di escludere terzi dall'ottenimento di tale accesso. La pena è la reclusione fino a 3 anni (Articolo 615 ter del codice penale).
- **Frode digitale**: si configura quando qualcuno manomette consapevolmente e con l'intento di frodare uno o più dispositivi digitali, utilizzando informazioni, dati o software per ottenere un guadagno economico o danneggiare qualcun altro. La pena è la reclusione da sei mesi a tre anni (Articolo 640 ter del codice penale).
- **Falsa identità**: il reato in questione è perpetrato quando qualcuno falsamente e volontariamente si sostituisce a qualcun altro. Si applica sia alle identità reali che a quelle digitali. La pena è la reclusione fino ad un anno (Articolo 494 del codice penale).
- **Detenzione e diffusione abusiva di password**: si verifica quando qualcuno intenzionalmente danneggia, distrugge, cancella o disabilita qualsiasi tipo di informazione digitale, dati o software di proprietà di qualcun altro. La pena è la reclusione da sei mesi a tre anni (Articolo 635 bis del codice penale).

Attacchi DOS

- **Danneggiamento di informazioni, dati o software**: il reato si configura quando qualcuno intenzionalmente danneggia, distrugge, cancella o disabilita qualsiasi tipo di informazione digitale, dati o software di proprietà di qualcun altro. Pena la reclusione da sei mesi a tre anni (Articolo 635 bis del codice penale).

Phishing

L'attacco tramite tecniche di phishing può produrre due tipi di reati già descritti:

- Frode digitale (Articolo 640 del codice penale).
- Falsa identità (Articolo 494 del codice penale).

Compromissione di sistemi IT con malware (ransomware, spyware, worm, trojan e virus)

I sistemi informatici si possono compromettere con malware tramite:

- Accesso abusivo ad un sistema informatico o telematico, già descritto sopra (Articolo 615 ter del codice penale).
- Danneggiamento di informazioni, dati o software, già descritto (Articolo 635-bis del codice penale).

Uso o mero possesso di hardware, software o altri strumenti utilizzati per commettere il crimine informatico e strumenti di hacking

- E' reato anche la detenzione e diffusione abusiva di **password** ai sistemi digitali (Articolo 615 quarto del codice penale).

Altre attività che minacciano la sicurezza, la riservatezza, l'integrità e la disponibilità di qualsiasi sistema IT, infrastrutture, reti di comunicazione, dispositivi o dati

- **Intercettazioni illegali e distruzione delle comunicazioni**: il reato è commesso quando una persona apre, ruba o distrugge la corrispondenza, comprese le e-mail, non indirizzate a lui o lei. La pena è la reclusione fino a un anno (Articolo 616 del codice penale).
- **Intercettazioni illegali, distorsione, falsificazione e distruzione delle comunicazioni**: questi diversi reati, puniti da diversi articoli del codice penale, sono commessi quando una persona apre, ruba o distrugge la corrispondenza altrui, comprese le e-mail, anche con software, malware o qualsiasi tipo di strumento digitale avente uno di questi scopi. La pena è della reclusione da sei mesi/un anno a quattro anni (Articolo 617 bis a 617 sexies del codice penale).
- **Divulgazione illecita di e-mail**: tale ipotesi di reato si configura nel caso in cui un soggetto intenzionalmente divulghi, o cerchi di divulgare, a qualsiasi altro soggetto, il contenuto di qualsiasi comunicazione via cavo, verbale o elettronica, sapendo o avendo motivo di sapere che l'informazione è stata ottenuta mediante intercettazione via cavo, verbale o elettronica in violazione della presente disposizione. La pena è la reclusione fino a sei mesi (Articolo 618 del codice penale).

Altri rischi che preoccupano le aziende italiane

Il report del **World Economic Forum** mostra un chiaro cambio di percezione del rischio legato ai sistemi e alle tecnologie informatiche da parte dei manager d'azienda italiani ed europei.

Italy	Cyberattacks	Critical information infrastructure breakdown	Manmade environmental catastrophes	Food crises	Data fraud or theft

Le aziende italiane sono preoccupate in modo particolare rispetto al resto del mondo dai rischi informatici, ma anche da altre minacce, quali i fenomeni naturali e catastrofali, la cui frequenza è progressivamente aumentata negli anni, con grossi impatti sul territorio e sugli asset di famiglie e imprese. Non si tratta di paure infondate: **il 91% dei comuni** è **a rischio di frane, allagamenti e**

alluvioni e **il 78% delle proprietà immobiliari** è **a rischio idrogeologico**, stando al rapporto Ispra 2018. In Italia, sembrano pesare anche gli **eventi catastrofali dovuti a una cattiva gestione o a comportamenti umani scorretti**: questi rischi si posizionano al terzo posto in Italia, mentre si trovano in coda alla classifica a livello europeo e mondiale.

Europe

Top ten risks in Europe

1. Cyberattacks
2. Asset bubble
3. Interstate conflict
4. Energy price shock
5. Fiscal crises
6. Data fraud or theft
7. Failure of national governance
8. Unemployment or underemployment
9. Large-scale involuntary migration
10. Profound social instability

A screen displays an eye at an electronics fair in Berlin, Germany. REUTERS/Hannib

Il **cambiamento climatico** e l'importanza sempre più pervasiva della **tecnologia** rientrano tra i timori comuni dei manager a livello europeo e mondiale. Per far fronte ai rischi legati al cambiamento climatico emerge la necessità di una collaborazione tra "pubblico-privato" in grado di prevenire, e intervenire, a tutela di famiglie e imprese. Relativamente al rischio tecnologico, il nostro Paese risulta scoperto in termini sia di preparazione e comprensione del rischio sia di capacità di affrontarlo, risulta quindi fondamentale un'azione diffusa di valutazione del **rischio cyber** soprattutto in soccorso delle **piccole e medie imprese**, che sono i soggetti tipicamente maggiormente esposti ai rischi informatici.