XVIII LEGISLATURA

PROPOSTA DI PIANO NAZIONALE DI RIPRESA E RESILIENZA
(DOC. XXVII, N. 18)

Introduzione

- **Trend Micro, leader globale di cybersecurity specializzata in soluzioni di sicurezza per i dati enterprise, i datacenter, gli ambienti cloud, le reti e gli endpoint, è una multinazionale con sedi principali a Tokyo e in Texas, e con sedi regionali e centri di Ricerca e Sviluppo in Asia, Europa e Nord America**. Con quasi 7.000 dipendenti in oltre 65 Paesi, Trend Micro opera in Italia dal 1998 ed è presente sul territorio con due sedi, una a Milano e una a Roma,

- Oltre 30 anni di esperienza nella security e nel campo della ricerca sulle minacce, con una propensione all'innovazione continua, hanno consentito a TM di rendere Istituzioni, aziende e persone cyber resilienti grazie a soluzioni connesse che proteggono i workload cloud, gli endpoint, le email, i dispositivi IIoT (Industrial Internet of Things) e le reti. **Nostro fiore all'occhiello, inoltre, è Trend Micro Research, una divisione specializzata in Ricerca e Sviluppo e nella lotta al cybercrime, che ci permette di detenere e usufruire della rete di intelligence sulle minacce più avanzate al mondo**.

- **Proprio dall'ultimo report sviluppato in piena emergenza pandemica da Trend Micro Research è emerso come l'Italia sia il quinto paese al mondo più colpito da macro malware**. Negli ultimi mesi, e complice anche l'emergenza dovuta al Covid-19, abbiamo infatti assistito ad un sostanziale incremento degli attacchi macro malware bloccati da TM, con Powload che si conferma il macro malware di maggior rilievo.

Questi numeri sono stati rilevati dalla **Trend Micro Smart Protection Network**, la rete intelligente e globale di TM che individua e analizza le minacce e aggiorna costantemente il database online relativo agli incidenti cyber, per bloccare gli attacchi in tempo reale. Grazie a questo processo **la nostra rete è in grado di bloccare una media di 65 miliardi di minacce all'anno.**
In particolare da gennaio a giugno 2020 Trend Micro ha potuto rilevare quasi 9 milioni di minacce legate al Covid-19. Queste minacce consistevano in e-mail, URL e file dannosi che facevano riferimento alla pandemia sia direttamente (ad esempio, un'app che pretendeva di fornire informazioni su Covid-19) o indirettamente (come i ritardi nella fornitura di servizi a causa del virus).

- Dobbiamo rilevare come, **benché oggi nel nostro Paese si senta spesso parlare di reti, innovazione e infrastrutture digitali, non si riesca tuttavia a porre la giusta attenzione sulla cyber security**. In questo ambito certamente si sono fatti passi avanti in termini di regolamentazioni e direttive sia a livello europeo che nazionale, ma il problema, che realtà come Trend Micro riscontrano quotidianamente, è una **scarsa consapevolezza dell'importanza che ricopre oggi nel Mondo la sicurezza cibernetica**.
  Quest'ultima continua ad essere vista come una commodity o semplicemente un adempimento necessario per rispondere a direttive o certificazioni, il tutto però nella costante **sottovalutazione dei danni che un attacco informatico e la conseguente perdita di dati sensibili o blocco generato alle attività può comportare** anche in termini produttivi, economici e sociali.

- Ecco perché collaboriamo ormai da anni con diverse Istituzioni nel sostenere lo sviluppo dell'innovazione tecnologica e dell'educazione agli strumenti digitali, nella convinzione che il nostro impegno possa apportare un contributo concreto alle politiche sociali, educative ed economiche del Paese.
  Siamo convinti, inoltre, che nel prossimo futuro si dovrebbe trovare il modo, anche a livello politico con norme ad hoc, di **coinvolgere maggiormente la parte apicale delle aziende pubbliche e private per aumentare l'attenzione** su questa tematica che è ormai diventata fondamentale per la protezione del sistema Paese.

PNRR e Digitale

- **Riteniamo di condividere le misure di supporto e sostegno al digitale e all'innovazione del sistema produttivo, soprattutto in relazione al Piano Transizione 4.0**, che vengono previste nella proposta di Piano Nazionale di Ripresa e di Resilienza.

  Investimenti in cyber security, l'implementazione delle reti ad altissima capacità e 5G, l'efficientamento del cloud nazionale e l'interoperabilità delle banche dati della PA, sono tutte misure ben in linea con gli obiettivi di innovazione e digitalizzazione più volte ribaditi in sede europea.

  Le tecnologie digitali, infatti, mentre cambiano diversi aspetti della nostra società, dallo smart working alla didattica a distanza, dall'intrattenimento alle relazioni sociali, condizionano sempre più i processi economici e organizzativi delle aziende e della Pubblica Amministrazione.

- **Il digital workplace se da un lato ha rappresentato e continuerà a rappresentare una grande opportunità di sviluppo e di crescita per le aziende, dall'altro comporterà unevitabile aumento dei rischi legati agli attacchi informatici**.

  La maggior parte delle aziende e delle Pubbliche Amministrazioni, infatti, si sono dimostrate impreparate a presidiare correttamente il telelavoro. Sono pochissime le imprese che hanno istruito per tempo il proprio personale nel rispettare alcune regole fondamentali a supporto della cybersecurity domestica.

  L'adozione di questo nuovo modello di lavoro richiede infatti un elevato livello di attenzione ai temi della cyber security. Non si tratta semplicemente di collegarsi in remoto alle risorse aziendali, ma di adottare un modello di lavoro completamente diverso.

  Anche per questo durante il lockdown i lavoratori hanno sviluppato un livello di consapevolezza sul fronte della sicurezza informatica molto più elevato rispetto al passato. Le criticità iniziano però quando le consapevolezze sulla cyber security devono tradursi in comportamenti concreti.

  Sono le aziende che, in un momento in cui la cyber security è finalmente riconosciuta dai dipendenti come fondamentale, devono investire sulla propria sicurezza cibernetica, insistere sulla formazione e potenziare le competenze, rivalutando, se necessario, le soluzioni messe a disposizione dei dipendenti che utilizzano le reti domestiche per accedere ai dati corporate.

- **Dalla protezione dei dati personali alla sicurezza cibernetica, sono molteplici i nodi emersi dal primo "esperimento" di scuola digitale forzato dal lockdown**.
  La necessità di assicurare la continuità didattica ha portato inevitabilmente a sottovalutare l'importanza di garantire un buon livello di tutela dei dati personali e ridurre al massimo i rischi di attacchi cyber.
  Rischi che nel contesto attuale della formazione a distanza aumentano esponenzialmente, soprattutto in virtù dell'utilizzo massivo di applicazioni e "social" sui device personali da parte dei giovani studenti.
  È fondamentale cominciare a pensare a percorsi di "educazione al digitale" non solo per i docenti ma anche per genitori e figli con una particolare attenzione alla cybersecurity e alla tutela della privacy nell'utilizzo delle applicazioni mobili.
  Così come sarebbe opportuno fornire agli istituti scolastici i sistemi operativi e le piattaforme DAD sicure e conformi al GDPR.

- **Siamo convinti che investendo sugli strumenti e le competenze digitali, la Pubblica Amministrazione e tutto il tessuto produttivo possano rendere sempre più efficienti, innovativi e interconnessi i servizi pubblici e privati dedicati ai cittadini**, sempre nel rispetto degli standard internazionali in materia di sicurezza e di tutela della privacy.

Osservazioni

- Le nostre riflessioni e osservazioni a questo punto non possono non convergere sulla parte del PNRR inerente alla missione e alle linee progettuali relative alla Digitalizzazione.
  La crescita digitale del nostro Paese passa inequivocabilmente proprio dalle misure che riusciremo a convogliare all'interno del nostro Piano Nazionale di Ripresa e Resilienza che presenteremo all'UE, una crescita però che non può essere legata esclusivamente ad aspetti tecnologici. Fondamentale sarà a questo proposito curare gli aspetti di educazione e di formazione, di sviluppo delle competenze e dei fattori abilitanti all'utilizzo delle nuove tecnologie.
  E la cyber security dovrà rappresentare uno dei fattori abilitanti

fondamentali.

- Ogni politica pubblica che andrà in questa direzione non potrà mai prescindere da una **modifica dell'organizzazione e dei processi tecnologici oggi esistenti nella PA e nelle aziende**. Necessario dunque investire sulle **competenze digitali** in tutti i settori della società e per una formazione riqualificante per i dipendenti pubblici e privati che metta al centro del sistema la cyber security.
  Un cambio di paradigma che vedrà necessariamente **l'upsklling e il reskilling digitali** dei dipendenti diventare sempre più centrali nel nuovo sistema.
  Solo così il digitale e la sicurezza cibernetica potranno rappresentare uno strumento concreto di ottimizzazione in termini economici e di miglioramento dei servizi ai cittadini.

- Accanto a questo sarà prioritario pensare a un **programma di educazione al digitale**, che consenta di accrescere le competenze dei cittadini, delle famiglie e soprattutto dei minori sia in termini di corretto impiego degli strumenti tecnologici sia in termini di promozione dell'uso consapevole della rete e dei diritti e doveri legati all'utilizzo di essa.

- Con la diffusione delle nuove tecnologie, infatti, si moltiplicano i relativi rischi legati agli attacchi informatici e alla gestione di tutti quei dati sensibili che rilasciamo sulla rete.
  L'emergenza sanitaria ha mostrato con sempre maggiore forza come la cyber resilienza sia imprescindibile per potere continuare a garantire i servizi anche in condizioni di crisi.
  In generale, e gli ultimi casi di attacchi a imprese molto note sul mercato lo dimostrano.
  Appare ormai evidente come la sicurezza cibernetica debba diventare non solo uno dei pilastri dell'attività di un'organizzazione pubblica e privata ma anche il **presupposto necessario di un'architettura nazionale di rete agile, evoluta e flessibile per il futuro**.

- Ecco perché il PNRR dovrebbe prevedere una **strategia per la sicurezza cibernetica sistemica**, con risorse non solo per l'acquisto di strumenti per la protezione di PA e aziende, ma anche per la formazione e l'educazione dei dipendenti, dei giovani e dei genitori, e per le attività di Ricerca e Sviluppo nella lotta al cyber crime.

- Dobbiamo rilevare l'urgente necessità di **investire nella sicurezza cibernetica e nell'attività di intelligence relativa alle minacce**. Conoscere, decrittare e anticipare la minaccia è la condizione essenziale e necessaria per scongiurare il rischio di essere colpiti.
  È fondamentale quindi che il PNRR sviluppi **un piano di investimenti e strategie per la cyber security che coinvolga l'intero sistema, pubblico e privato, economico e sociale.**
  Sarebbe opportuno dunque cominciare da un insieme chiaro e definito di procedure e norme a cui gli enti pubblici e le aziende che trattano dati sensibili dovranno conformarsi per proteggere i propri sistemi.

- La pandemia con la conseguente diffusione dell'utilizzo degli strumenti digitali, ha mostrato come il concetto di prevenzione del rischio di attacchi cyber sia assolutamente mutato, passando dal semplice presidio del perimetro aziendale alla necessità di monitorare un orizzonte sempre più esteso, fatto di reti pubbliche, private e domestiche. Da qui il dovere di modernizzare l'intero Paese sul tema della Cyber Security, portando la cyber resilienza a diventare **l'elemento fondante e abilitante di tutti i servizi, piattaforme e applicazioni digitali**.
  Il PNRR dovrebbe quindi prevedere misure di cyber security per ogni missione e linea progettuale relative alla Digitalizzazione, precisando voci e interventi specifici.
  Soprattutto se pensiamo alla tanto agognata transizione al cloud, non si potrà non tenere conto dell'esigenze di cyber sicurezza relative alla data protection, anche grazie a "certificazioni di security".

- Per rafforzare la filiera della Cyber Security sarebbe auspicabile, inoltre, prevedere l'obbligo per imprese e PA (compresi gli istituti scolastici) di adottare **prodotti, strumenti e tecnologie "hack proof"**, e di dotarsi della figura di **Chief Information Security Officer (CISO)** e, per determinati contesti, di certificazioni «accountable» (es. ISO 27001).
  A questo proposito il PNRR dovrebbe contemplare lo **stanziamento di risorse per l'ammodernamento informatico dei sistemi IT delle PA** per porre rimedio all'obsolescenza dei sistemi attuali che utilizzano tecnologia facilmente aggredibile dall'esterno.

Nel settore privato, invece, è imprescindibile a questo fine la previsione dell'**aumento, almeno fino al 50%, dell'agevolazione fiscale del credito d'imposta sull'acquisto di software, sistemi, piattaforme e applicazioni per la protezione di reti, dati, programmi, macchine e impianti da attacchi, danni e accessi non autorizzati**.

- Nella stessa direzione si dovrebbe **aumentare il credito d'imposta per gli investimenti in Ricerca e Sviluppo** per raccogliere informazioni, dati, analisi e soluzioni relative alle minacce cyber e agli strumenti per combatterle.

- Come detto in precedenza e come speriamo di aver posto alla vostra attenzione, i recenti casi di cronaca con attacchi massivi ad aziende molto famose ribadiscono l'importanza di investire nella sicurezza cibernetica.
  Le risorse del PNRR rappresentano una irripetibile opportunità che abbiamo il dovere di non sprecare, perché solo così potremmo iniziare una rivoluzione tecnologica e culturale che permetterà un cambio di paradigma nella prevenzione dei rischi legati agli attacchi informatici.