# La cybersicurezza nazionale: la nuova frontiera della difesa dello Stato

***Gaetana Natale****

Difendere i confini del proprio Stato significa oggi difendere lo spazio cibernetico: il passaggio dal territorio al cloud ci impone di innalzare il livello di alert, in quanto il diffondersi delle connessioni digitali ha aumentato la c.d. superficie di attacco. Ma in che modo e con quali strumenti?

Di recente sono state fornite istruzioni precise alle pubbliche amministrazioni per cambiare le soluzioni dedicate alla sicurezza degli endpoint e al firewall che venivano fornite da provider legati alla Russia, i quali potrebbero non essere in grado di fornire aggiornamenti e soluzioni a causa della guerra in Ucraina, con possibili ripercussioni sul sistema di sicurezza nazionale.

Si tratta di sei best practice da attuare per evitare rischi, contenute nella circolare numero 4336 del 21 aprile 2022 dell'Agenzia per la cybersicurezza nazionale (1) in attuazione dell'articolo 29, comma 3 del cosiddetto Decreto Ucraina, cioè il decreto numero 21 del 21 marzo 2022.

La norma prevede infatti che le PA sostituiscano i prodotti di sicurezza informatica di operatori legati alla Russia, in quanto, a causa del conflitto in corso, i provider potrebbero non aver la possibilità di "*fornire servizi e aggiornamenti ai propri prodotti*", si legge nella circolare pubblicata in Gazzetta Ufficiale il 26 aprile.

---

(*) Avvocato dello Stato, Professore a contratto di Sistemi Giuridici Comparati, Consigliere giuridico del Garante per la Privacy.

***Redazione delle note a cura della Dott.ssa Anna Pagano, ammessa alla pratica forense presso l'Avvocatura Generale dello Stato.***

(1) L'adozione del D.L. 14 giugno 2021, n. 82 ha ridefinito l'architettura nazionale cyber e istituito l'Agenzia per la Cybersicurezza Nazionale (ACN) a tutela degli interessi nazionali nel campo della cybersicurezza. L'ACN è Autorità nazionale per la cybersicurezza e assicura il coordinamento tra i soggetti pubblici coinvolti nella materia. Promuove la realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica necessarie allo sviluppo digitale del Paese. Persegue il conseguimento dell'autonomia strategica nazionale ed europea nel settore del digitale, in sinergia con il sistema produttivo nazionale, nonché attraverso il coinvolgimento del mondo dell'università e della ricerca. Favorisce specifici percorsi formativi per lo sviluppo della forza lavoro nel settore e sostiene campagne di sensibilizzazione oltre che una diffusa cultura della cybersicurezza. Sull'istituzione dell'ACN si veda: A. Macrì, "*Agenzia per la cybersicurezza nazionale e PNRR*" su *actedmagazine.com*; "*Agenzia per la Cybersicurezza Nazionale: cos'è e come funziona*" su *https://www.insic.it/privacy-e-sicurezza/information-security/al-via-lagenzia-per-la-cybersicurezza-nazionale/*; "*Agenzia per la cybersicurezza nazionale: via libera del Governo Draghi*" su *https://www.ancdv.it/web/index.php?option=com_content&view=article&id=724:acn-agenzia-per-la-cybersicurezza-nazionale-via-libera-del-governo-draghi&catid=114&Itemid=1180*; "*Come cambia la sicurezza cybernetica in Italia*" su *https://www.cybersecitalia.it/agenzia-cybersicurezza-nazionale-ecco-il-logo-sito-web-e-al-via-campagna-reclutamento-cyber-defender/15919/*.

All'origine della circolare c'è un approccio risk based: sono individuate sei buone pratiche da realizzare immediatamente, ma soprattutto invita le PA ad agire sia nel controllo di quanto in esercizio che nell'acquisto di nuove tecnologie, con metodi risk based, ossia partendo sempre da una analisi del rischio.

Con il Decreto Ucraina, relativo a "*Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina*", il Governo ha evidenziato la necessità di rafforzare le difese. In particolare, il citato comma 3 dell'articolo 29 del decreto prevede per le PA la "*diversificazione dei prodotti di sicurezza informatica in uso*" forniti dai provider legati alla Russia, "*al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici*". Effetti che possono essere conseguenza dell'impossibilità, da parte dei provider, di aggiornare le soluzioni o fornire i propri servizi, proprio a causa della guerra.

La circolare spiega che i prodotti di cui si parla nel decreto sono quelli relativi a:

- endpoint security, compresi antivirus, antimalware ed EDR
- WAF - web application firewall.

In particolare, vengono citati nella circolare i prodotti delle società Kaspersky Lab (2), Group IB e i prodotti di Positive Technologies rispettivamente nel comma 3 dell'articolo 29 alla lettera A per le prime due aziende e alla lettera B per la terza società.

***Le sei raccomandazioni dell'Agenzia per la cybersicurezza nazionale.***

La circolare riporta sei raccomandazioni per "*adottare tutte le misure e le buone prassi di gestione di servizi informatici e del rischio cyber e, in particolare, di tenere conto di quanto definito dal Framework nazionale per la cybersecurity e la data protection, del 2019, realizzato dal Centro di ricerca di cyber intelligence and information security (CIS) dell'Università Sapienza di Roma e dal Cybersecurity national lab del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorità garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza*" (3).

---

(2) La società Kaspersky Lab, fondata in Russia nel 1997 da Eugene e Natalya Kaspersky, è divenuta famosa nel mondo per i suoi sistemi antivirus. In questo momento storico, però, con il protrarsi della guerra in Ucraina l'affidabilità di tali sistemi è stata fortemente messa in discussione per il rischio che tale società venga sfruttata per diffondere malware o spyware all'interno delle infrastrutture in cui è istallato. Sul punto si vedano i seguenti articoli: "*Il caso Kaspersky ci racconta come siamo in pericolo (digitale)*" su *https://www.panorama.it/Tecnologia/cyber-security/kaspersky-russia-spionaggio-hacker*; Per una prospettiva comparata: "*Caso Kaspersky: le mosse di Italia, Francia e Olanda a confronto*" su *https://www.startmag.it/innovazione/caso-kaspersky-le-mosse-di-italia-francia-e-olanda-a-confronto/*; "*Kaspersky e software russi via dai dispositivi della PA italiana, la circolare dell'ACN*" su *https://www.corriere.it/economia/cybersecurity-aziende-privati-evento/notizie/kaspersky-software-russi-via-dispositivi-pa-italiana-circolare-dell-acn-70ee28bc-c7ab-11ec-8e7f-1a021a80175d.shtml.*

È da ricordare l'importanza della Convenzione di Budapest sulla criminalità informatica. Di recente il Consiglio di Europa ha adottato una decisione che autorizza gli Stati membri a firmare nell'interesse dell'UE il secondo protocollo addizionale alla Convenzione suddetta. Questo protocollo migliorerà l'accesso transfrontaliero alle "prove elettroniche" da utilizzare nei procedimenti penali. Contribuirà alla lotta contro la criminalità informatica a livello mondiale, semplificando la cooperazione tra gli Stati membri e i paesi terzi, garantendo un elevato livello di protezione delle persone e il rispetto delle norme UE in materia di protezione dei dati. Attualmente 66 paesi di cui 26 Stati membri dell'UE sono parti della Convenzione di Budapest, che, oltre a rafforzare la cooperazione diretta con i prestatori di servizi, stabilisce le c.d. procedure per la mutua assistenza giudiziaria di emergenza.

---

(3) Circolare del 21 aprile 2022, n. 4336. Attuazione dell'articolo 29, comma 3, del decreto-legge 21 marzo 2022, n. 21. Diversificazione di prodotti e servizi tecnologici di sicurezza informatica. (22A02611) (GU Serie Generale n. 96 del 26-04-2022) su *https://www.gazzettaufficiale.it/eli/id/2022/04/26/22A02611/sg.*
A) Premessa.
"Con il decreto-legge 21 marzo 2022, n. 21, recante «Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina», il Governo ha ritenuto, tra l'altro, la straordinaria necessità e urgenza di assicurare il rafforzamento dei presidi per la sicurezza, la difesa nazionale, le reti di comunicazione elettronica e degli approvvigionamenti di materie prime. A tale riguardo, l'art. 29, comma 1, del medesimo decreto-legge, prevede che, al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, derivanti dal rischio che le aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Federazione Russa non siano in grado di fornire servizi e aggiornamenti ai propri prodotti, in conseguenza della crisi in Ucraina, le medesime amministrazioni procedano tempestivamente alla diversificazione dei prodotti in uso.
Più nello specifico, il medesimo art. 29, secondo il combinato disposto dei commi 1 e 3, prevede che l'individuazione dei prodotti e servizi da diversificare avvenga in relazione alle categorie indicate con circolare dell'Agenzia per la cybersicurezza nazionale tra quelle volte ad assicurare le seguenti funzioni di sicurezza: *a)* sicurezza dei dispositivi (*endpoint security*), ivi compresi applicativi *antivirus*, *antimalware* ed «*endpoint detection and response*» (EDR); *b)* «*web application firewall*» (WAF).
La presente circolare è volta, pertanto, ad indicare le categorie di prodotti e servizi tecnologici di sicurezza informatica per le quali le pubbliche amministrazioni dovranno procedere a diversificazione ai sensi dell'art. 29, del decreto-legge n. 21 del 2022.
B) Individuazione dei prodotti e servizi oggetto di diversificazione.
Ai fini dell'individuazione dei prodotti e servizi tecnologici di sicurezza informatica di aziende produttrici legate alla Federazione Russa, ai sensi dell'art. 29, commi 1 e 3, del decreto-legge n. 21 del 2022, ciascuna pubblica amministrazione destinataria della presente circolare procede alla diversificazione delle seguenti categorie di prodotti e servizi tecnologici di sicurezza informatica:
1) prodotti e servizi di cui all'art. 29, comma 3, lettera *a)*, del decreto-legge n. 21 del 2022, della società «Kaspersky Lab» e della società «Group-IB», anche commercializzati tramite canale di rivendita indiretta e/o anche veicolati tramite accordi quadro o contratti quadro in modalità «*on-premise*» o «da remoto»;
2) prodotti e servizi di cui all'art. 29, comma 3, lettera *b)*, del decreto-legge n. 21 del 2022, della società «Positive Technologies», anche commercializzati tramite canale di rivendita indiretta e/o anche veicolati tramite accordi quadro o contratti quadro in modalità «*on-premise*» o «da remoto».
C) Raccomandazioni procedurali.
Si raccomanda alle amministrazioni destinatarie della presente circolare - responsabili nella conduzione delle operazioni di configurazione dei nuovi servizi e prodotti acquisiti ai sensi dell'art. 29 del decreto-legge n. 21 del 2022, anche in relazione alla precisa conoscenza dei propri *asset* (reti, sistemi informativi

Le sei best practice della Circolare:

1. Censire prodotti e servizi indicati nella circolare e analizzare "*gli impatti degli aggiornamenti degli stessi sull'operatività, quali i tempi di manutenzione necessari*";

2. Individuare nuovi servizi e prodotti e farne una valutazione, considerando sia che siano compatibili con i propri asset e la "*complessità di gestione operativa delle strutture di supporto in essere*";

3. Occuparsi della definizione, condivisione e comunicazione dei piani di migrazione;

4. Validare i modi per eseguire il piano di migrazione "*su asset di test significativi, assicurandosi di procedere con la migrazione dei servizi e prodotti sugli asset più critici soltanto dopo la validazione di alcune migrazioni e con l'ausilio di piani di ripristino a breve termine al fine di garantire la necessaria continuità operativa*", spiega la circolare. Si chiarisce anche che il piano di migrazione "*dovrà garantire che in nessun momento venga interrotta la funzione di protezione garantita dagli strumenti oggetto della diversificazione*";

---

e servizi informatici) e degli impatti degli stessi sulla continuità dei servizi e della protezione dei dati - di adottare tutte le misure e le buone prassi di gestione di servizi informatici e del rischio *cyber* e, in particolare, di tenere conto di quanto definito dal *Framework* nazionale per la *cybersecurity* e la *data protection*, edizione 2019, realizzato dal Centro di ricerca di *cyber intelligence and information security* (CIS) dell'Università Sapienza di Roma e dal *Cybersecurity national lab* del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorità garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza.

In particolare, si raccomanda di:

1) censire dettagliatamente i servizi e prodotti di cui al paragrafo *B)* della presente circolare, analizzando gli impatti degli aggiornamenti degli stessi sull'operatività, quali i tempi di manutenzione necessari;

2) identificare e valutare i nuovi servizi e prodotti, validandone la compatibilità con i propri *asset*, nonché la complessità di gestione operativa delle strutture di supporto in essere;

3) definire, condividere e comunicare i piani di migrazione con tutti i soggetti interessati a titolo diretto o indiretto, quali organizzazioni interne alle amministrazioni e soggetti terzi;

4) validare le modalità di esecuzione del piano di migrazione su *asset* di test significativi, assicurandosi di procedere con la migrazione dei servizi e prodotti sugli *asset* più critici soltanto dopo la validazione di alcune migrazioni e con l'ausilio di piani di ripristino a breve termine al fine di garantire la necessaria continuità operativa. Il piano di migrazione dovrà garantire che in nessun momento venga interrotta la funzione di protezione garantita dagli strumenti oggetto della diversificazione;

5) analizzare e validare le funzionalità e integrazioni dei nuovi servizi e prodotti, assicurando l'applicazione di regole e configurazioni di sicurezza proporzionate a scenari di rischio elevati (quali, ad esempio, autenticazione multi-fattore per tutti gli accessi privilegiati, attivazione dei soli servizi e funzioni strettamente necessari, adozione di principi di «zero-trust»);

6) assicurare adeguato monitoraggio e audit dei nuovi prodotti e servizi, prevendendo adeguato supporto per l'aggiornamento e la revisione delle configurazioni in linea.

Nella predisposizione, migrazione e gestione dei nuovi prodotti e servizi, si raccomanda l'adozione di principi trasversali di indirizzo, quali a titolo esemplificativo quello della «gestione del rischio», in termini di identificazione, valutazione e mitigazione dei rischi di diversa fattispecie che concorrono nell'attuazione della diversificazione dei servizi.

Infine, si raccomanda alle amministrazioni di controllare costantemente i canali istituzionali di comunicazione dell'Agenzia per la cybersicurezza nazionale https://www.acn.gov.it/ e https://csirt.gov".

5. Condurre analisi e validazione delle funzioni e integrazioni dei nuovi prodotti e servizi scelti, "*assicurando l'applicazione di regole e configurazioni di sicurezza proporzionate a scenari di rischio elevati*". Tra questi rientrano autenticazione multi fattore per ogni accesso privilegiato, attivare solo funzioni necessarie e adottare principi di zero-trust;

6. Garantire monitoraggio e audit dei nuovi prodotti, con la previsione di un adeguato sostegno per gli aggiornamenti e le revisioni delle configurazioni.

Considerando questi consigli si deduce che l'analisi del rischio è la metodologia base di una postura consapevole e pronta rispetto alla minaccia cyber. Ormai tutte le metodologie sposate dalle amministrazioni occidentali partono dalla analisi del rischio. L'Europa è profondamente consapevole di questo e si sta muovendo in tal senso in tutte le proposte di nuove direttive (come la NIS 2 e la CER). La postura cyber sicura è prima di tutto una postura risk based basata sulla c.d. awarness, consapevolezza delle potenzialità di attacco.

***Il ruolo dell'Agenzia di cybersicurezza nazionale.***

Stiamo vivendo un momento storico senza precedenti, in cui ci troviamo per la prima volta a dover agire tempestivamente per arginare un rischio cyber importante legato ad una crisi geo politica in atto. Emerge, quindi, non solo l'importanza di avere un ente deputato alla gestione del tema, l'Agenzia di cybersicurezza nazionale guidata dalla figura autorevole del prof. Baldoni, ma anche la sua efficacia. Questa circolare chiarisce in modo inequivocabile i prodotti già valutati dall'Agenzia, nell'ottica delle raccomandazioni fornite dallo CSIRT Italia prima e dal Decreto legislativo 21/22, così come chiesto da diverse organizzazioni. Vengono inoltre fornite precise indicazioni sul come procedere alla diversificazione dei prodotti e servizi informatici.

***L'impatto del contesto politico.***

Per comprendere la rilevanza delle decisioni in questo ambito, è importante considerare il contesto geo politico attuale. La decisione dell'Agenzia è motivata dal fatto che nell'ottica di rafforzamento della postura di sicurezza informatica nazionale è necessario mitigare il rischio derivante dall'indisponibilità di prodotti e servizi tecnologici forniti da aziende di sicurezza informatica legate alla Federazione Russa (4). Nella circolare si evidenzia come

(4) La guerra in Ucraina non è infatti solo una guerra sul campo ma passa anche attraverso attacchi cyber tanto da definire questa come una guerra cybernetica. Basti pensare al fatto che i primi attacchi hacker al sistema ucraino sono avvenuti intorno al 13 gennaio, più di un mese prima dell'inizio ufficiale della guerra. Per rispondere a tali attacchi, in seguito il gruppo Anonymous ha dato vita ad una serie di hackeraggi effettuati a vari siti governativi nonché alla Banca Centrale della Federazione Russa. Il famoso gruppo non è l'unico a combattere contro la Russia ma ce ne sono anche altri come il gruppo polacco Squad303 e il bielorusso Cyber Partisan, oppositore del Presidente Lukashenko. Per un

queste aziende possano non essere in grado di fornire servizi e aggiornamenti ai propri prodotti.

In un contesto internazionale come quello attuale caratterizzato da notevoli tensioni geopolitiche è fondamentale distinguere la decisione politica da quella tecnologica e acquisire la consapevolezza del livello di rischio di un attacco informatico di tipo DDos (Denial of Service), elemento attivo di minaccia concreta alle istituzioni e infrastrutture critiche. Bisogna prestare massima attenzione anche alla dimensione digitale dei conflitti prima che sfocino in veri e propri casus belli: una sorta di attentato di Sarajevo digitale. *Si vis pacem para bellum* significa oggi potenziare la c.d. "robustezza" della sicurezza digitale.

La circolare della ACN evidenzia la necessità di affrontare il rischio dell'attacco informatico: è significativo osservare che la circolare suddetta non qualifica il rischio di utilizzo degli stessi servizi e prodotti come vettore di attacco, bensì mette in luce la loro indisponibilità legata al conflitto. Prevale un'impostazione condivisibile non belligerante, ma tesa a garantire la sicurezza dei sistemi informatici preposti all'erogazione dei servizi pubblici essenziali del paese.

La circolare emanata dall'ACN rafforza il concetto di sovranità tecnologica nazionale e della necessità nel tempo di rendere le nostre infrastrutture critiche indipendenti dalle tecnologie straniere (5). Altro aspetto cruciale è la capacità di qualifica di sistemi hardware e software che importiamo. Dobbiamo sviluppare una capacità di analisi tale da rendere ragionevolmente sicura l'adozione di queste soluzioni da parte delle nostre imprese e della pubblica amministrazione (6).

---

approfondimento si veda: *https://www.repubblica.it/esteri/2022/03/24/news/anonymous_e_la_guerra_cibernetica_in_ucraina_domande_e_risposte_per_capire_gli_attacchi_degli_hacker-342704238/*; *https://www.cybersecurity360.it/nuove-minacce/guerra-cibernetica-gli-impatti-del-conflitto-russia-ucraina-e-il-contrattacco-di-anonymous/*; *https://www.wired.it/article/ucraina-russia-guerra-ransomware-conti/ ;https://www.redhotcyber.com/post/la-cybergang-russa-oldgremlin-attacca-le-aziende-russe/* ; *https://www.huffingtonpost.it/esteri/2022/04/27/news/ucraina_microsoft_da_hacker_russi_ondata_di_cyber_attacchi-9276132/.*

(5) Nel decreto legislativo attualmente in discussione, l'ACN viene individuata come autorità nazionale di certificazione di cyber security di prodotto al fine di adeguare il sistema nazionale al quadro europeo (*https://www.cybersecurity360.it/outlook/certificazioni-di-cyber-security-il-futuro-nel-decreto-in-arrivo/*).

(6) Ciò è necessario soprattutto alla luce dei molteplici attacchi informatici subiti da aziende pubbliche e private nei campi più disparati. Da ultimo, si segnala il recentissimo attacco cyber avvenuto a diversi siti italiani tra i quali, il sito istituzionale del Senato, della Difesa, della Scuola alti studi di Lucca, l'Istituto superiore di Sanità, da parte del gruppo russo Killnet (*https://www.rainews.it/articoli/2022/05/attacco-hacker-ai-siti-di-senato-e-difesa-rivendicato-dal-gruppo-russo-killnet-e8495f90-7a5f-44bb-8512-bb63c4b39e5d.html*). Invece, nella notte tra il 30 aprile e il 1 maggio 2022 i sistemi informatici dell'Ospedale Fatebenefratelli Sacco di Milano sono stati vittima di un attacco haker che ha provocato notevoli disservizi che incidono inevitabilmente sulle cure dei pazienti (*https://www.cybersecurity360.it/nuove-minacce/ransomware/attacco-informatico-allasst-fatebenefratelli-sacco-di-milano-potrebbe-essere-un-ransomware/; https://quifinanza.it/innovazione/video/ospedali-in-tilt-nuovo-attacco-hacker-colpisce-italia-cosa-sappiamo/646091/* ). Le strutture sanitarie sono quelle più al rischio perché sempre più sotto il mirino degli attacchi hacker, basti pensare all'attacco di tipo ransomware subito nel 2021 dal sistema sanitario

Secondo eu-Lisa (Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia) che ha sede a Tallin (7) è importante una mappatura delle infrastrutture critiche con un'attività di prevenzione per attuare il c.d. "disaster recovery" con cloud nazionale "robusto" dal punto di vista della sicurezza nazionale. Sono determinanti il c.d. controll vulnerabilities e i sistemi di notification, perché molto spesso gli atti informatici sono silenziosi e non facilmente individuabili (8). Un attacco informatico può spesso determinare un effetto spill-over su altri computer portando ad un completo blocco di tutti i sistemi informatici con danni inestimabili. Ecco perché si sta definendo la figura del cibersecurity specialist, figura inizialmente sviluppatasi in Israele con competenze trasversali volta a prevenire incidenti ed attacchi informatici che possono determinare un arresto improvviso di tutti i servizi essenziali di un paese. Il controllo del mondo digitale

---

irlandese o da quello neozelandese o quelli avvenuti in ospedali americani (*https://www.lastampa.it/cronaca/2021/05/14/news/irlanda-attacco-hacker-al-sistema-sanitario-1.40270603/ ; https://www.wired.it/internet/web/2021/05/25/ospedali-hacker-nuova-zelanda-irlanda-ransomware/; https://www.cybersecurity360.it/nuove-minacce/ransomware/irlanda-attacco-ransomware-al-sistema-sanitario-cosa-imparare-ancora-dalle-lezioni-del-passato/* ). Gli attacchi perlopiù si sostanziano in attacchi ransomware che si caratterizzano per la scansione dei file importanti e per un processo di crittografia avanzato non reversibile, paralizzando un'organizzazione più velocemente di altre applicazioni dannose. In Italia, attacchi di questo tipo hanno riguardato enti come la Regione Lazio i cui sistemi informatici hanno riportato non pochi danni data l'interruzione dei servizi che ne è conseguita per quasi un mese (*https://www.pandasecurity.com/it/mediacenter/sicurezza/attacco-regione-lazio/, https://www.cybersecurity360.it/nuove-minacce/regione-lazio-vaccini-bloccati-poco-pronta-contro-il-ranwomare-ecco-perche/*); ma anche le Ferrovie dello Stato che nel mese di marzo 2022 ha rilevato, durante i controlli di sicurezza giornalieri, elementi che riconducono ad un attacco di crytolocker. FS ha poi deciso in via precauzionale di disattivare alcune utenze dei sistemi di vendita fisici, tutti i sistemi di self service utilizzati nelle varie stazioni, mentre è rimasta attiva la vendita online (*https://www.insic.it/privacy-e-sicurezza/information-security/attacco-hacker-alle-ferrovie-dello-stato-tutti-i-dettagli/*). Sempre con riguardo agli attacchi ransomware, un nuovo gruppo di questo tipo, ribattezzato Black Basta e già noto per aver recentemente preso di mira l'American Dental Association (ADA), è arrivato anche in Italia. Si tratta di un malware che ruba i dati delle vittime e li cripta sfruttando servizi leciti di Windows (*https://www.cybersecurity360.it/nuove-minacce/ransomware/black-basta-il-ransomware-che-sfrutta-i-servizi-di-windows-per-criptare-i-dati-i-dettagli/* ). Ad esser presa di mira dagli attacchi cybernetici sono anche società private come la Coca-Cola, la quale è stata vittima di un attacco in cui sono stati sottratti 161 GB di dati, poi messi in vendita per 1,65 bitcoin (*https://sicurezza.net/cyber-security/coca-cola-stormous-ruba-161gb-di-dati/#gref* ). Il Governo degli Stati Uniti, per cercare di far fronte "all'emergenza hacker", ha deciso di istituire una taglia di 10 milioni di dollari per coloro i quali siano in grado di fornire informazioni che possano portare alla cattura o quanto meno all'identificazione del famoso gruppo hacker Conti. (*https://www.computermagazine.it/2022/05/10/conti-il-gruppo-hacker-ha-le-ore-contate-taglia-di-10-milioni-di-dollari-dal-governo-usa/*).

(7) Il Gruppo Leonardo ha vinto il contratto per gestire la sicurezza delle infrastrutture It e delle sedi della struttura eu-Lisa. L'accordo, della durata di cinque anni, prevede servizi di cyber security integrati erogati da specialisti di Leonardo a protezione di tutte le sedi di eu-Lisa (*https://www.milanofinanza.it/news/a-leonardo-la-cyber-security-dell-agenzia-europea-lisa-202205060939498036).*

(8) Sotto l'aspetto della sicurezza delle aziende sono rilevanti anche i sistemi VPN. Tuttavia, sono state messe in luce alcune criticità che possono rilevare alcuni elementi di vulnerabilità. Sul punto: "*VPN e se la sicurezza fosse apparente?*" (*https://www.cybersecurity360.it/outlook/vpn-e-se-la-sicurezza-fosse-apparente-ecco-la-soluzione*/).

è determinante per la sicurezza di un paese: di questo il governo italiano è pienamente consapevole, avendo previsto il sistema del golden power (con obbligatorietà della notifica al governo) per tutte le imprese straniere che manifestino la propria volontà di acquisire partecipazioni azionarie in società italiane coinvolte nella realizzazione del 5 G.

Friedrich Nietzsche parlava di Wille zur Macht per indicare la cieca tendenza degli organismi a espandersi a detrimento del circostante, nonché la necessità di dominare, occupare, sottomettere. Oggi tale desiderio di dominio avviene nello spazio cibernetico: occorrono competenze, consapevolezza e strategie per realizzare un sistema di sicurezza nazionale che ci metta al riparo da attacchi informatici insidiosi e pericolosi: è la nuova frontiera della difesa digitale dei nostri sistemi democratici.