Il Sole 24 ORE

diffusione:105722
tiratura:156556

Il paradosso italiano tra digitale e sicurezza

Il piano «Industria 4.0» offre alle aziende una netta occasione per investire in innovazione. Più fosca la visione sulla cybersecurity

di **Alessandro Longo**

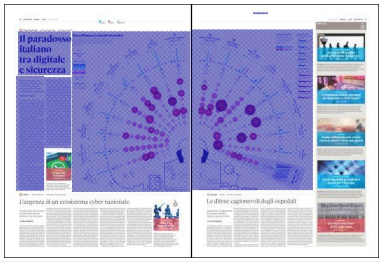
Una industria nazionale innovativa deve essere anche cyber sicura, gli esperti sono concordi; ma su questo punto l'Italia sta procedendo con uno strabismo che non ha pari nella storia del digitale. Da una parte, «abbiamo probabilmente, con l'ultima Legge di Bilancio, il piano Industry 4.0 più completo in Europa», dice Andrea Bianchi, direttore Politiche Industriali di Confindustria. Dall'altra, abbiamo anche il piano cybersecurity più misero tra i grandi Paesi europei, per risorse impiegate e ampiezza della strategia.

Il paradosso è emerso durante l'evento Itasec questa settimana, a Venezia, e sarà toccato il 25 gennaio a Roma all'Industry 4.0 Summit alla Camera dei Deputati. «Piano Industry 4.0 e strategia cybersecurity devono viaggiare di pari passo, altrimenti quelli del piano non saranno solo investimenti sprecati, ma rischiano persino di trasformarsi in un boomerang per le aziende», riassume Paolo Prinetto, presidente del Cini, Consorzio Interuniversitario Nazionale per l'Informatica (organizzatore di Itasec con l'università Ca' Foscari di Venezia). Consideriamo infatti che Industry 4.0 significa, tra l'altro, tanta intelligenza in più nelle nostre fabbriche: sensori, robot, software.

Laddove ci sono software e connessioni ci possono essere vulnerabilità informatiche: si amplia di tanto la superficie d'attacco. Non preoccuparsi di difenderla in modo adeguato significa esporsi a rischi enormi. È un po' come se le repubbliche marinare del medioevo avessero potenziato le navi mercantili senza fare crescere di pari passo la flotta navale a protezione. Sarebbe stata una bella pacchia per i pirati. Informatici, nel nostro caso. Il mondo l'ha già capito: infatti, secondo Gartner, la spesa complessiva globale per la sicurezza in ambito Internet delle cose è stata di 348 milioni di dollari nel 2016, in crescita di circa il 24% rispetto al 2015.

Per fortuna il piano Industry 4.0 non ignora del tutto il tema cyber security. Vi dedica un capitolo (sebbene senza risorse specifiche). «Indirettamente, Industry 4.0 aiuterà la cyber security nazionale perché incentiva anche gli investimenti in software, che possono essere quelli di sicurezza», dice Alvise Biffi, presidente Assolombarda e vice presidente Piccola Industria Confindustria e fondatore di Secure Networks. «La difficoltà sarà veicolare sui piani aziendali cybersecurity gli incentivi possibili con Industry 4.0, dato che la sicurezza non è solo una questione di nuovi software ma richiede anche cambi organizzativi e di processo, nuove competenze», aggiunge Biffi. Un ruolo in tal senso lo potranno svolgere le associazioni di settore e i competence center, previsti dal piano Industry 4.0 (anche se per ora con molte meno risorse di quelle annunciate dal Governo e con obiettivi poco definiti).

«In Confindustria stiamo sviluppando un modello che traduca il framework della cybersecurity nazionale (elaborato dal Cini) in azioni semplici, alla portata di tutte le aziende», dice Biffi. Sarà uno strumento gratuito in forma di modulo web, dove le aziende saranno guidate passo passo per capire il proprio livello di esposizione al rischio informatico e cosa fare per rimediare. «Sarà pronto per marzo. E sarà facile da usare, anche per le aziende meno tecnologiche», dice Biffi. «La sfida principale sarà aiutare le nostre tante Pmi, dove le competenze tecnologiche sono bassissime, a crescere in innovazione e sicurezza assieme, nei



Il Sole 24 ORE

diffusione:105722
tiratura:156556

prossimi anni», conferma Presidente della Sezione Servizi Innovativi e Tecnologici di Confindustria Vicenza, che sta organizzando corsi specifici per Industry 4.0, sul territorio, con un modulo dedicato alla cybersicurezza.

«I nuovi pericoli informatici obbligano le aziende a fare un salto culturale: devono investire su tecnologie per la prevenzione del rischio; mentre finora si sono limitate a predisporre solo sistemi per reagire alle minacce che emergevano di volta in volta», ha detto a Itasec Mauro Palmigiani, country manager dell'azienda di sicurezza digitale Palo Alto Networks. Tra l'altro, da maggio 2018 si aggiunge anche la scure delle sanzioni (fino al 4% di fatturato) previste dal nuovo regolamento europeo privacy, se si subisce un accesso abusivo ai dati personali trattati dall'azienda. Avverte Prinetto: «Se le aziende investiranno in innovazione ma non in sicurezza potranno essere attaccate con facilità, certo; ma non solo: espongono a rischi anche i clienti che usano i loro prodotti. Ne deriva per le aziende un grosso danno di credibilità ed economico».

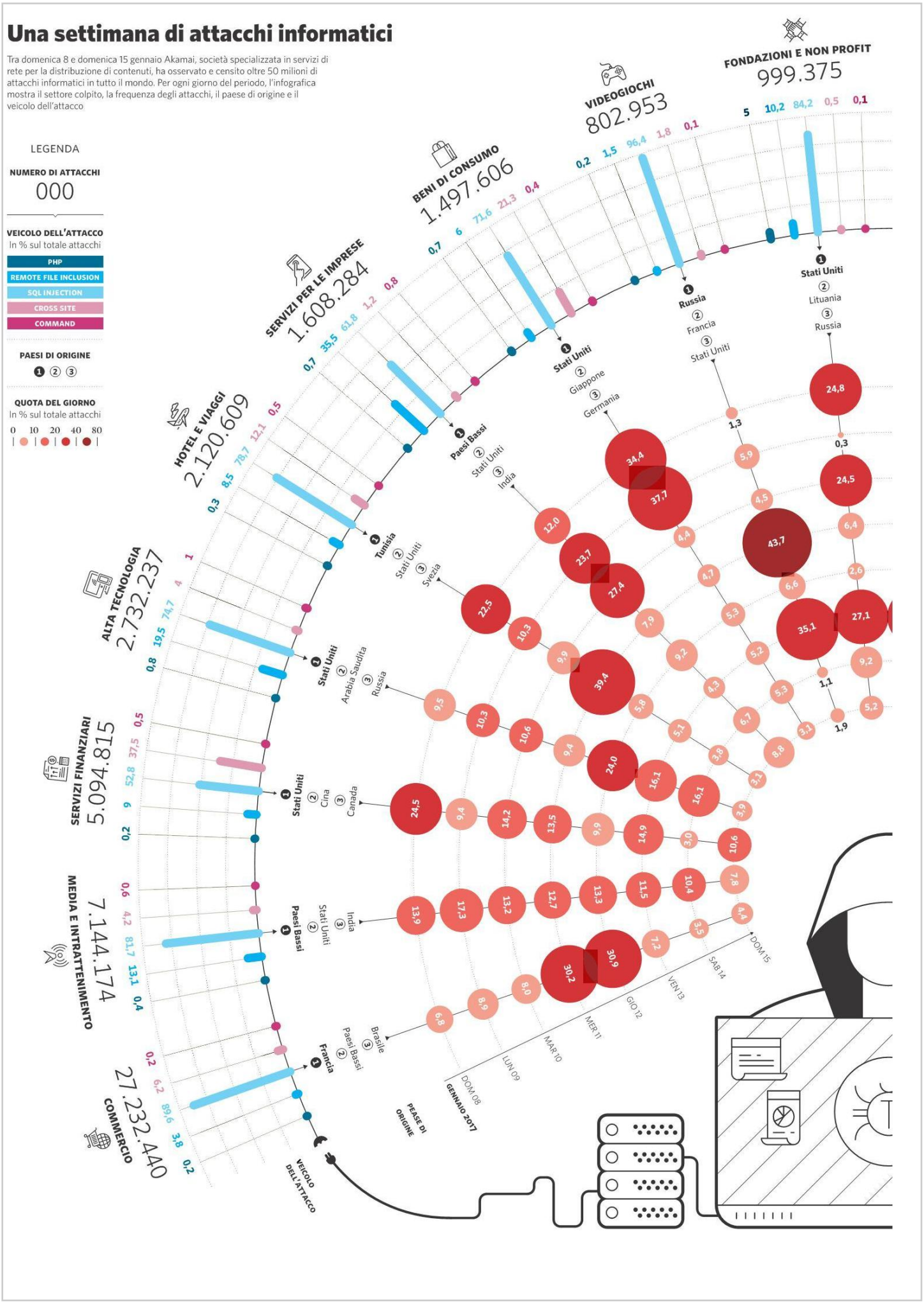
@AlessLongo

Il Sole 24 ORE

diffusione:105722
tiratura:156556

Una settimana di attacchi informatici

Tra domenica 8 e domenica 15 gennaio Akamai, società specializzata in servizi di rete per la distribuzione di contenuti, ha osservato e censito oltre 50 milioni di attacchi informatici in tutto il mondo. Per ogni giorno del periodo, l'infografica mostra il settore colpito, la frequenza degli attacchi, il paese di origine e il veicolo dell'attacco



Il Sole 24 ORE

diffusione:105722
tiratura:156556