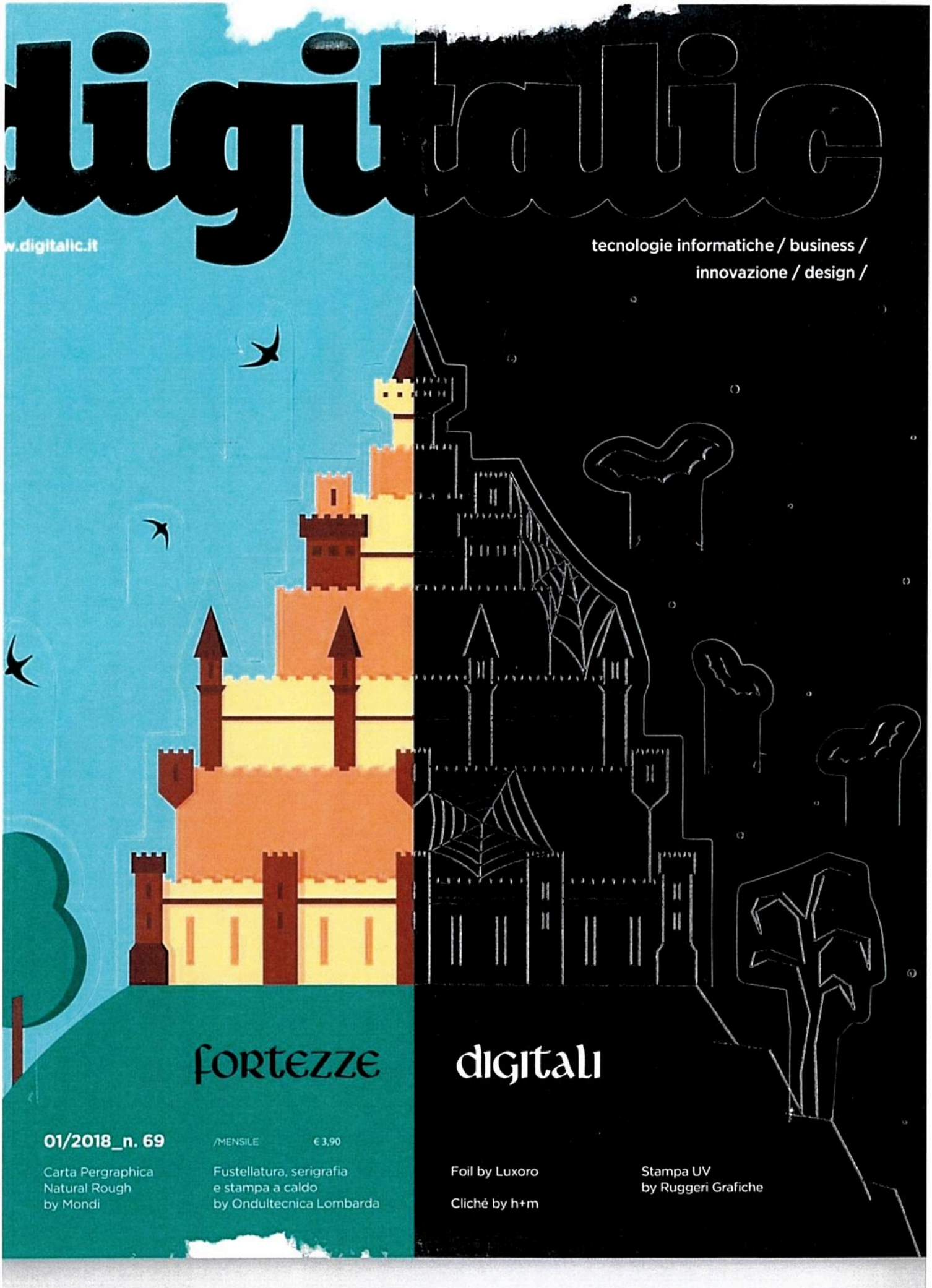
digitalic

www.digitalic.it

tecnologie informatiche / business /
innovazione / design /



fortezze digitali

01/2018_n. 69 /MENSILE € 3,90

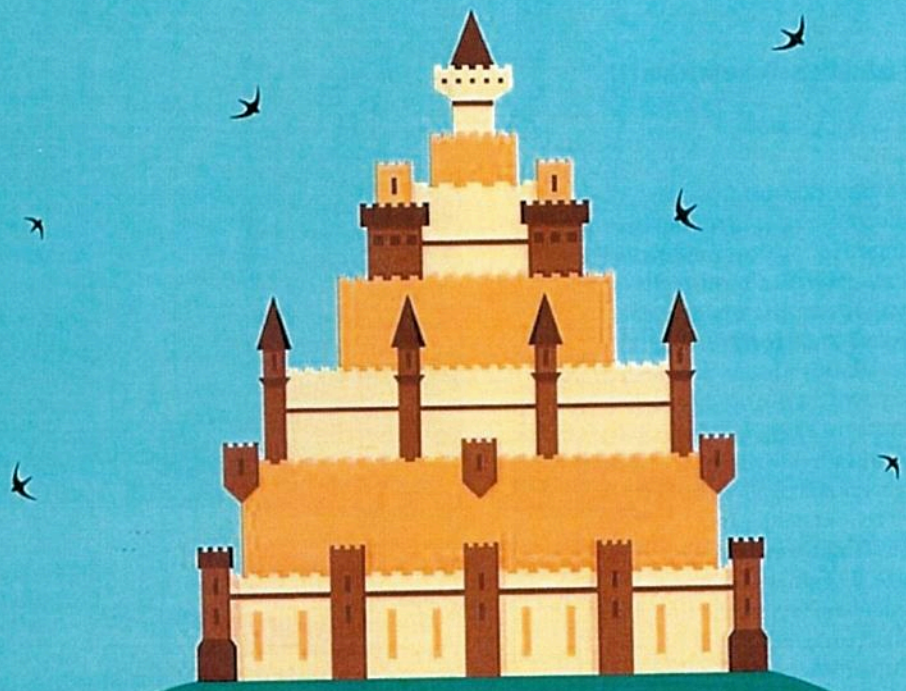
Carta Pergraphica
Natural Rough
by Mondi

Fustellatura, serigrafia
e stampa a caldo
by Ondultecnica Lombarda

Foil by Luxoro

Cliché by h+m

Stampa UV
by Ruggeri Grafiche



MINACCE DIGITALI: COME PROTEGGERSI, TRA TECNOLOGIA E STRATEGIA

Il cloud computing, i dispositivi mobili sempre più avanzati, la disponibilità di banda e l'IoT hanno cambiato il modo di lavorare della gente, ma nel contempo rappresentano un terreno sempre più fertile (e per certi versi sterminato) per furti, frodi e attività criminali.

A cura della redazione

Oggi non c'è aspetto della vita umana e lavorativa che non sia collegato con l'universo digitale. Con l'avanzare della trasformazione, quindi, il vero rischio per le aziende di tutte le dimensioni sarà sempre più l'allargamento del perimetro da proteggere e l'enorme mole di informazioni generata giorno per giorno. Con i principali player del settore abbiamo analizzato pericoli più diffusi e strategie per proteggersi.

Quali sono le minacce digitali più diffuse oggi?

Per prima cosa non bisogna sottovalutare i ransomware, secondo Andrea Muzzi, Sales Engineer F-Secure. "Nel 2017 sono state scoperte nuove famiglie ransomware e varianti come mai nel passato. L'epidemia Wannacry dello scorso maggio è stata la più grande della storia e per il 2018 ci si attende che le aziende dovranno affrontare attacchi mirati. Anche l'Internet of Things rappresenta sempre più un tema dibattuto dal punto di vista della mancanza di sicurezza dei dispositivi connessi a Internet. Non solo. Molta importanza riveste ancora il fattore umano. La cultura verso un uso consapevole delle tecnologie rappresenta ancora una parte fondamentale nella sicurezza globale delle aziende e della vita di ognuno di noi. Molti degli attacchi che vengono sferrati si basano ancora sul fattore umano, sfruttano la poca cultura nella gestione del rischio informatico".
Lo conferma Gastone Nencini, Country Manager Trend Micro Italia: "Sono in crescita le truffe Bec (Business Email Compromise). In questa tipologia di attacco si spinge un dipendente a effettuare l'accredito di una grossa somma di denaro a un conto cybercriminale spacciandosi il più delle volte per il Ceo. I settori aziendali più colpiti sono ovviamente quelli amministrativi e molti dipendenti, vedendosi arrivare una richiesta del proprio superiore confezionata ad arte, cadono nel tranello. Queste truffe hanno successo perché il rischio è molto basso in relazione alla possibile somma di denaro che si ottiene. Nell'ultimo periodo abbiamo notato anche truffe Bpc (Business Process Compromise), ove la compromissione avviene a livello di processo all'interno dell'azienda. Un esempio può esser quello relativo alla sostituzione al momento della stampa del codice Iban sulle fatture inviate ai clienti".
Domenico Raguseo, Manager of Europe Technical Sales, IBM Security, ricorda che i rischi dipendono da molti

essere d'accordo: sicuramente l'intelligenza artificiale è un'opportunità fino a che non va a impattare la privacy o la vita stessa delle persone.
Andrea Muzzi di F-Secure, specifica: "Dal punto di vista della sicurezza informatica sarà sempre di più una risorsa fondamentale e vincente. L'intelligenza artificiale giocherà un ruolo importantissimo, garantendo efficacia e grande velocità nella risposta. Tuttavia al giorno d'oggi l'intelligenza artificiale non può garantire da sola la totale sicurezza. L'intervento umano risulta ancora un tassello fondamentale. Sul fatto che possa rappresentare una minaccia, il dibattito è aperto. Molte delle menti della Silicon Valley hanno espresso preoccupazione per il rapido sviluppo dell'AI. Avrà un impatto sulla nostra vita quotidiana. Non si può frenare lo sviluppo tecnologico, ma sicuramente si può eticizzare".
Domenico Tizzano di Dedagroup, racconta che il suo team, per difendere le organizzazioni con i propri servizi gestiti, si avvale di tools sviluppati ad-hoc e in continua evoluzione, che raccolgono e analizzano le informazioni fondamentali prodotte dalle tecnologie di sicurezza adottate dai clienti e che rendono l'operato degli analisti sempre più rapido e puntuale. I tools utilizzano diverse tecnologie di AI e Machine Learning, supervisionate da un umano. Questo perché l'ultima decisione non può – ancora - essere demandata alla macchina.
Carmelo Garofalo di SAS, prosegue: "In un contesto così dinamico e complesso è necessario cambiare paradigma e transitare da un approccio reattivo a un approccio proattivo, dove l'intelligenza artificiale, nelle sue varie declinazioni, rappresenta un'opportunità importante per supportare gli analisti di sicurezza informatica. Oggi nelle organizzazioni la maggior parte dei controlli e delle analisi avviene mediante la realizzazione di regole deterministiche disegnate ed implementate in modo manuale dagli analisti o da correlatori tradizionali, come i Siem. Visto la dinamicità, la complessità ed il volume di alert che possono essere generati è necessario andare verso un approccio risk-based, dove un motore di intelligenza artificiale, attraverso algoritmi e modelli di machine learning, elabora centinaia o milioni di eventi di sicurezza in modo automatico, individuando da un lato pattern di attacco non noti, individuabili con le regole di correlazione tradizionali e, dall'altro, prioritizzando gli alert generati mediante il calcolo di uno score di rischio dinamico sull'entità analizzata, considerando il numero di risorse limitato presenti nelle varie organizzazioni".
Domenico Raguseo di IBM Security, conferma: "L'Intelligenza Artificiale o, come preferiamo chiamarla in IBM, l'Intelligenza Aumentata è una opportunità per chi difende, in quanto aumenta la produttività, l'efficacia e la competenza degli analisti di sicurezza. Infatti la soluzione IBM Watson for Cyber Security integra funzionalità cognitive che, comprendendo il linguaggio naturale, rendono possibile interpretare le potenziali minacce all'interno della moltitudine di dati non strutturati (come quelli di social media, articoli, blog, notizie) attualmente non gestiti e non gestibili dall'uomo".
Mirko Gatto di Var Group conclude: "L'intelligenza artificiale è fra le emerging technology quella che senza dubbio sta rivoluzionando di più il nostro futuro. come ogni nuova opportunità, essa nasconde chiaramente molteplici minacce. La questione non è tanto fidarsi o meno dell'Intelligenza Artificiale, quanto piuttosto continuare a non fidarsi di chi possa sfruttare ogni mezzo per arrecare danno e mettere a repentaglio il patrimonio informativo aziendale. Nella divisione cybersecurity di Var Group abbiamo già integrato l'AI nello sviluppo di progetti, anche per realizzare una chatbot che permette ai clienti di interrogare il Security Operation Center senza utilizzare un linguaggio tecnico".

Il canale italiano è preparato a sostenere le imprese nella lotta al cybercrime? Su cosa dovrebbe investire un rivenditore?

Luca Casini di V-Valley, dice che "l'entrata in vigore a livello europeo della Gdpr (General Data Protection Regulation) rappresenta un'opportunità da non perdere in tema di sicurezza. Il nostro obiettivo è aiutare i rivenditori nel riuscire a sfruttarla al meglio e creare valore. A tale scopo stiamo organizzando eventi con studi legali e professionisti che collaborano con le istituzioni nella stesura dei regolamenti. Inoltre, siamo in grado di affiancare i rivenditori con i nostri team di supporto pre-vendita, offrendo consulenze su misura per trovare le soluzioni più adatte ad ogni realtà aziendale.
Un altro tema promettente è sicuramente l'IoT poiché offre svariate potenzialità di business, ma va affrontato in modo adeguato, per capire come integrare le sue diverse declinazioni. Sicuramente, sta nascendo la necessità di collaborazione tra diversi operatori, che sviluppino soluzioni, impieghino i sistemi informativi e sappiano gestire la sensoristica. Per questo, stiamo avviando un progetto volto a generare collaborazione tra i rivenditori per offrire ai mercati soluzioni integrate".
Luca Casini conclude: "V-Valley è certamente pronta a supportare i rivenditori nella lotta al cybercrime. L'integrazione di Mosaico va proprio in questa direzione. Siamo infatti riusciti a creare un vero e proprio 'Hub del valore' a servizio dei rivenditori, in grado di abbracciare tutti i mega trend dell'Ict – Cybersecurity in primis ma anche Cloud IoT, Iperconvergenza – con una gamma ampia e completa, un team di specialisti che hanno competenze, esperienza e abilità nel parlare la lingua del rivenditore, servizi di formazione e la capacità di rispondere a tutte le esigenze di mercato". ■

Stefano Sordi, Aruba

Tino Canegrati, HP Italy

Valerio Rosano,
ZyXEL Communications

Mirko Gatto,
Var Group