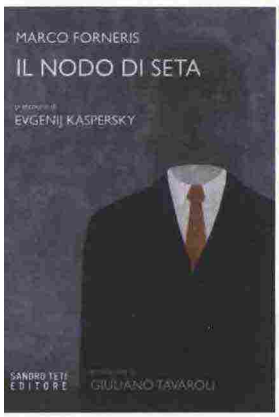
Tiratura: 8.000 Diffusione: 7.500

SISTEMI &IMPRESA

Mensile

Data 10-2017
Pagina 72
Foglio 1

I LIBRI DEL MESE



Marco Forneris

IL NODO DI SETA

Editore: Sandro Teti Editore
Prima edizione 2016
pp. 343, € 16,00

Viviamo in un'epoca nella quale i cyber attacchi sono ormai all'ordine del giorno. Con l'espansione delle Reti e con i device sempre connessi, nessuno è dunque più al riparo. Secondo l'ultimo rapporto di Europol (l'ufficio europeo di polizia), sono circa 2 miliardi i dati e le informazioni sottratti ai cittadini europei e divulgati sul web. Inoltre nell'ultimo anno è stato segnalato l'aumento esponenziale dei gruppi di malware che hanno reso vulnerabili i dispositivi elettronici (+750%). Nel mirino dei cyber criminali internazionali, come ha segnalato l'Europol, ci sono le banche e le grandi imprese. È proprio una banca al centro de *Il nodo di seta*, primo romanzo di Marco Forneris, che in carriera ha ricoperto il ruolo di Chief Information Officer (CIO) di alcune grandi aziende italiane: nel libro si racconta di un attacco informatico a un istituto di credito, con una trama che si complica ancora di più quando, oltre alla frode informatica, si intrecciano misteriosi omicidi.

A firmare la prefazione è Evgenij Kaspersky, fondatore dell'omonima azienda leader mondiali nella produzione di antivirus, che propone interessanti approfondimenti sul tema, evidenziando soprattutto come i criminali siano abili a sfruttare l'anello debole di tutta la filiera: l'uomo. Il thriller di Forneris, infatti, trae spunto da fatti realmente accaduti, riplasmandoli e trasformandoli in un romanzo che, seppur vicino alla realtà, a volte se ne discosta, ma non troppo (per esempio è noto che all'inizio del Terzo Millennio il cyber crime non era ancora così esteso come oggi, nonostante ci fossero già le tecnologie adeguate), arrivando addirittura all'ombra del Cupolone...

Protagonista del thriller è David Faure, incaricato dalla Allgemeine Bank di Francoforte di indagare sulla sparizione di quasi 450 milioni di dollari dai conti offshore della banca privata Sutter. Faure si mette a capo di un team per svolgere l'indagine (a volte anche con mezzi non convenzionali) e mettersi sulle tracce della verità, in un viaggio che lo porterà da Lugano a Roma, dai Caraibi a New York, da Tallinn a Mosca fino a Gerusalemme per inseguire imprenditori spregiudicati, hacker quasi invisibili, spie israeliane fino ad alti prelati vaticani.

Scrive Kaspersky: "Nel 2014 abbiamo aiutato diverse banche dell'Europa dell'Est ad affrontare attacchi informatici: abbiamo scoperto una banda di hacker che aveva messo in atto nel tempo, con tutta probabilità, la più grande rapina bancaria della Storia". Ciò che sconvolge, però, è nel prosieguo: "Procedendo con le indagini, abbiamo scoperto che il primo software usato per il furto era stato messo a punto dalla banda nel 2013, quasi un anno prima che il gruppo criminale riuscisse a sgraffignare soldi alle sue vittime". In pratica è la descrizione di un tipico attacco informatico: un impiegato riceve una email con un file allegato che apparentemente sembra innocuo, invece contiene il malware che, una volta aperto, consente di installare sul pc una backdoor. È da qui che i criminali avranno accesso alla rete dell'azienda, con tutto il tempo per raccogliere dati e informazioni sull'organizzazione e i clienti. "La triste realtà odierna è che quasi tutto ciò che si serve di un computer è connesso alla Rete ed è basato su un software che contiene punti deboli, a volte persino migliaia, e alcuni di questi possono essere sfruttati dai pirati informatici", ammette Kaspersky.

Caustico il commento del guru di cyberwar e cyberterrorismo: "Nel mondo ci sono due tipi di aziende, quelle che sono state attaccate e quelle che non lo sono state... finora". Di quale fate parte?