della stessa collana

SECURITY E PRIVACY

CYBERSECURITY & CYBERWARFARE

Michele Iaselli, Giovanni Battista Caria

gli autori

Diritto, tecnologia e sicurezza

vai alla scheda del libro

EPC EDITORE

Michele Iaselli, Giovanni Battista Caria

CYBERSECURITY & CYBERWARFARE

Diritto, tecnologia e sicurezza

EPC EDITORE

CYBERSECURITY E CYBERWARFARE: DIRITTO, TECNOLOGIA E SICUREZZA
ISBN: 978-88-9288-194-5

EPC S.r.l. Socio Unico – Via Clauzetto, 12 – 00188 Roma – www.epc.it
Servizio clienti: 06 33245277/271 – clienti@epc.it
Redazione: 06 33245264/205

Il codice QR che si trova sul retro della copertina, consente attraverso uno smartphone di accedere direttamente alle informazioni di questo volume.
https://www.epc.it/Prodotto/Editoria/Libri/Cybersecurity-e-cyberwarfare-diritto-tecnologia-e-sicurezza/5198

Foto di copertina: www.123rf.com – monsit jangariyawong

SOMMARIO

PREFAZIONE

I recenti eventi bellici che coinvolgono direttamente la Russia e l'Ucraina, ma indirettamente l'intero nostro pianeta per le inevitabili conseguenze politiche, economiche e sociali hanno evidenziato la grande rilevanza che ormai sta assumendo la c.d. *cyberwar* da intendersi come l'utilizzo di computer e di reti per attaccare o difendersi nel cyberspazio.

La *cyberwar* è tipica della terza rivoluzione industriale (o postindustriale), come la guerra elettronica lo è stata della seconda. Possiede aspetti tecnico-operativi sia offensivi che difensivi e viene utilizzata sia in tempo di pace che nel corso di conflitti armati. Dal punto di vista offensivo, l'attacco cibernetico può utilizzare diverse tecniche e tattiche e proporsi diversi obiettivi: intercettazione di dati; inabilitazione delle reti e degli equipaggiamenti informatici nemici; attacco alle infrastrutture critiche (elettricità, gasdotti e oleodotti, rete delle telecomunicazioni commerciali e finanziarie, trasporti ecc.). Le modalità di attuazione degli attacchi vanno dal superamento dei sistemi protettivi e dall'entrata nelle reti informative e nelle banche dati, con finalità varie (dall'acquisizione di informazioni al vandalismo di *hacker* individuali), all'attacco massiccio condotto da unità specializzate, alla diffusione di virus informatici o di worm, per neutralizzare reti, sistemi d'arma o di comando, di controllo e di comunicazione.

Molti preferiscono parlare di *cyberwarfare* per esprimere meglio un concetto equivalente al "campo di battaglia digitale", un nuovo scenario nel quale la guerra fra Stati si sposta dal piano reale a quello virtuale. Usare il termine "virtuale" non deve però trarre in inganno. Nel mon-

do odierno praticamente tutti gli elementi della nostra vita dipendono da una qualche forma di strumento digitale: dai trasporti alla produzione dell'energia, dalla sanità alla comunicazione, dal lavoro allo svago. Attaccare le nostre infrastrutture digitali, impedendogli di funzionare correttamente, significa allora attaccare le nostre infrastrutture reali, in modo non dissimile a un attacco terroristico. Non stupisce quindi che la guerra si stia trasferendo sempre più su questo nuovo piano, creando scenari del tutto nuovi che richiedono conoscenze precise e misure adeguate alla minaccia.

Potremo dire che la guerra riflette i cambiamenti storici, le sue trasformazioni culturali e tecnologiche. La nuova frontiera dei conflitti fra stati è appunto il *cyberwarfare*. Il campo di battaglia è diventato la rete, mentre i soldati si sono trasformati in hacker.

La diffusione di documenti secretati operata da Edward Snowden, l'attacco alle centrali nucleari iraniane, le intromissioni russe nella campagna presidenziale americana del 2016: questi eventi ci mostrano una nuova figura di *hacker*, che agisce per conto di potenze straniere, che lavora in sincrono con altri, e che ha come obiettivo non più il guadagno personale, ma l'indebolimento di un intero apparato statale.

Nello specifico per *cyberwarfare* si intende:

1) *Attacco a infrastrutture:* si tratta di attacchi contro il sistema informatico che gestisce infrastrutture critiche per il funzionamento di uno stato, come i sistemi idrici, energetici, sanitari, dei trasporti e militari.

2) *Attacco ad apparecchiature:* questo tipo di attacco, più militare in senso classico, ha l'obiettivo di compromettere il funzionamento di sistemi di comunicazione militari come satelliti o computer.

3) *Guerriglia Web:* in questo caso l'attacco consiste in rapidi atti vandalici contro server e pagine web, creando più scompiglio che veri e propri danni informatici.

4) *Cyberspionaggio:* proprio come lo spionaggio classico, questa attività cerca di rubare informazioni sensibili, siano esse di carattere militare che aziendale, avendo spesso come obiettivo grandi compagnie nazionali.

5) *Propaganda:* questo tipo di attacco è più nascosto e subdolo: il suo scopo è quello di infondere dubbi nella popolazione e creare malcontento attraverso la divulgazione di messaggi politici e fake news, soprattutto attraverso i social.

Naturalmente per approfondire la conoscenza di questa nuova realtà è necessario conoscere bene quelle nozioni essenziali di cybersecurity e quindi cosa si intende per cyber risk, come è possibile difendersi da attacchi informatici o prevenire gli stessi. Inoltre negli ultimi tempi il nostro Paese ha concentrato la propria attenzione anche da un punto di vista normativo e quindi diventa fondamentale conoscere i principali interventi del legislatore in materia.

Naturalmente azioni informatiche che cagionano danni ad infrastrutture, sistemi informatici, dati, informazioni, si sostanziano nella maggior parte dei casi in veri e propri reati informatici disciplinati dal nostro codice penale e da leggi speciali ed è naturalmente opportuno conoscere la tipologia e disciplina dei principali reati in materia.

Talvolta come si è già avuto modo di anticipare la cyberwarfare comprende anche azioni di cyberspionaggio per cui è importante conoscere le principali nozioni di intelligence e come è organizzato il nostro Paese in questo settore molto delicato.

Non per ultimo la cyberwarfare pone problemi di regolamentazione in ambito internazionale e può estendersi ad una vera e propria forma di guerra spaziale con il coinvolgimento di satelliti spia per cui vanno approfondite anche tematiche di diritto internazionale dello spazio ancora poco conosciute.

L'obiettivo di questo libro è quindi proprio quello di fornire un quadro generale su tutti gli aspetti di natura tecnica, giuridica e sociale sottolineati e strettamente collegati alla cyberwarfare.

Si è ritenuto, inoltre, di arricchire il testo con delle testimonianze dirette di esperti informatici e giuristi che analizzano in concreto casi reali legati anche al conflitto Russia-Ucraina.

PARTE I

SEZIONE GIURIDICA

Di seguito riportiamo tutti gli autori che hanno contribuito alla PARTE I - Sezione giuridica

Fabrizio Corona, avvocato partner di e-lawyers consulenza legale, Docente di Intelligenza artificiale, machine learning e diritto presso università LUISS Guido Carli – Roma, Docente di Informatica Giuridica presso l'Università Telematica Giustino Fortunato – Benevento.

Piera Di Stefano, avvocato, si occupa di web reputation, crimini informatici e privacy. È co-fondatrice, unitamente all'avv. Michele Di Somma, del progetto «Avvocato del Web®», responsabile affari legislativi e istituzionali di Consumerismo no-profit, di cui è portavoce per la Cyber Security, e membro del comitato scientifico di ANDIP. Scrive per riviste e rubriche su reputazione on line, privacy e cybercrime ed è docente e co-autrice di testi su diritto e nuove tecnologie.

Gianpiero Uricchio, Dottore Commercialista esperto nelle attività relative al D.Lgs. 231/2001 e al Regolamento UE 679/2016 in materia di trattamento dei dati personali. Maestro della Protezione dei dati personali e Data Protection designer, iscritto all'albo dell'Istituto italiano Privacy. Professionista della Privacy presso ANORC. Cultore della materia del Trattamento dei dati personali e reati informatici, presso l'Università di Cassino. Membro della commissione 231 e Privacy dell'ODCEC di Napoli. Membro del Gruppo di esperti a supporto dell'EDPB in materia di nuove tecnologie.

Diego Padovan, Ingegnere dell'informazione, docente e ricercatore in data management e cyber security, ha ideato e portato sul mercato il primo ethical hacker virtuale.

Vittorio Iaselli, dottore in giurisprudenza specializzato presso la scuola delle professioni legali di Unicusano, consulente privacy. Maestro della Protezione dei dati personali e Data Protection designer, iscritto all'albo dell'Istituto italiano Privacy. Professionista della Privacy presso ANORC. Coautore di testi su diritto e nuove tecnologie.

capitolo 1

LA SICUREZZA INFORMATICA

di

Diego Padovan

Sommario: 1.1. Che cosa si intende per cyber risk. – **1.2.** L'evoluzione della rete, i rischi e gli attacchi informatici. – **1.3.** Il concetto di sicurezza informatica. – **1.4.** Le misure di sicurezza nel Regolamento europeo sulla protezione dei dati personali. – **1.5.** Come difendersi dai virus ed in particolare dalle nuove generazioni di virus.

1.1. Che cosa si intende per cyber risk

Il concetto di cibernetica si riferisce molto genericamente alle implicazioni nella vita quotidiana dei mondi virtuali, ovvero alle interazioni più o meno avanzate tra uomo e computer, con specifico riferimento all'ambiente internet, anche detto *online*.

Il *world wide web*, e più genericamente l'interconnessione tra oggetti che dialogano attraverso una rete condivisa, ha reso l'informazione la risorsa più importante. Il dato è l'elemento chiave e di scambio tra le macchine e le applicazioni ivi risiedenti nonché tra queste ultime e l'uomo, in un ciclo continuo e interattivo di arricchimento reciproco. Da un lato esse migliorano il servizio fornito all'utente, sia in termini di esperienza che di utilità, dall'altro l'informazione è utilizzata per soddisfare bisogni e consentire nuove modalità di utilizzo dell'ambiente cibernetico.

In ogni caso, lo scambio delle informazioni per qualsiasi persona e organizzazione necessita di alcune garanzie. In particolare, affinché il dato possa rappresentare un valore per l'ecosistema digitale, esso deve essere scambiato e reso disponibile preservandone la confidenzialità e l'integrità. Difatti, un dato indisponibile non rappresenta una risorsa per chi (sia esso uomo o macchina) necessita dei suoi elementi per portare a termine una o più attività. Similmente, un dato corrotto,

perché modificato senza un criterio o un permesso da parte di chi gestisce quel dato, non rappresenta più un valore per alcuno. Infine, nel caso in cui un dato necessiti di un certo livello di confidenzialità, se questa venisse a mancare ne conseguirebbe l'immediata perdita di valore o una ricaduta negativa nei confronti di coloro i quali il dato si riferisce (es., finanziaria, reputazionale, ecc.).

Riassumendo, i principi di integrità, confidenzialità e disponibilità sono i fattori chiave per la gestione in sicurezza dell'informazione. Detti fattori, noti anche come CIA *factors* (dall'inglese *Confidentiality, Integrity e Availability)*, sono pertanto gli elementi da considerare quando si individuano i parametri attraverso i quali si pianifica e si esegue una corretta impostazione della sicurezza informatica.

Di contro, data la complessità ormai raggiunta dall'ecosistema digitale, sussistono innumerevoli minacce ai fattori CIA e, di conseguenza, altrettante possibilità di perdita di valore del dato e del sistema che lo gestisce. Queste possibilità, per chi gestisce la security, sono analizzate congiuntamente agli impatti sui sistemi informatici e sulle informazioni qualora si concretizzino. Affinché ciò sia possibile, il primo passaggio è la corretta definizione di rischio cibernetico (in inglese *cyber risk).*

Internet e, più in generale, l'ecosistema digitale, offre molte opportunità e nuove minacce. Proprio per questo motivo, le domande che assillano gli utenti e le aziende che operano nel mondo digitale sono sempre riferibili ai fattori CIA. Infatti, sono prevalentemente riferibili a come sia possibile assicurare la confidenzialità, l'integrità e la disponibilità delle proprie risorse, con le quali operano nel mondo digitale.

Per fare alcuni esempi: l'informazione è custodita in maniera appropriata? Il sistema è affidabile o è già nelle mani di chi può sfruttarlo a fini malevoli? Cosa succederebbe se le informazioni non fossero più disponibili o accessibili quando necessario? Per trovare una risposta soddisfacente a queste domande, una delle strade più concrete è quella di procedere attraverso un processo di valutazione del rischio cibernetico.

L'analisi del *cyber risk* consiste nello stimare la probabilità che un evento avverso infici l'esperienza digitale dell'utente, così come dell'azienda nel suo complesso, prendendo in debita considerazione le implicazioni al verificarsi di tali occorrenze. Ciò significa capire qual è la probabilità che un danno derivante dalle risorse *online* si concretizzi.

Dal punto di vista matematico il rischio informatico è definito come la probabilità che un evento avverso si verifichi, moltiplicato per l'impatto che avrebbe questo evento sulle risorse informatiche gestite.

Comprendere questi due elementi che compongono il *cyber risk*, significa comprendere il valore delle risorse gestite (dati o informazioni), nonché la propria esposizione agli attacchi informatici. Infatti, semplificando, più si è esposti *online* e coinvolti nelle dinamiche dell'ecosistema digitale, più è probabile che un criminale informatico sia interessato ad ostacolare proprio queste attività, a proprio vantaggio (es. riscatti dovuti da ransomware). Di conseguenza, più è probabile che si sia oggetto di interesse da parte di hacker malintenzionati, più è alto l'impatto che un attacco può avere sul sistema informatico.

Per identificare i rischi relativi alla sicurezza delle informazioni, quelli associati alla perdita di riservatezza, integrità e disponibilità delle informazioni, è necessario seguire un approccio tanto più rigoroso quanto più è complesso ed articolato il sistema informatico da tutelare e quanto più preziose sono le informazioni ivi presenti. Solo in questo modo sarà possibile procedere con la ponderazione del rischio, comparando lo stato attuale, grazie ai risultati dell'analisi ottenuti mediante dei criteri definiti precedentemente, con i risultati desiderati (anche noti in inglese come *desired state*). Tale processo porta ad identificare uno scostamento (anche noto come GAP) rispetto ad un ideale quadro di sicurezza informatica che tiene conto della specifica realtà cui si applicherebbe. Il passo successivo è l'individuazione delle priorità di trattamento del rischio.

Il processo di valutazione del rischio viene attuato in fase di revisione o di sviluppo di un sistema di gestione della sicurezza informatica (tra i più noti quello legato alla norma ISO 27001) e riesaminato almeno su base annuale. Inoltre, il processo è eseguito anche ogni qual volta ci siano variazioni rilevanti di tipo tecnico, normativo od organizzativo che impattano sui rischi relativi alla sicurezza delle informazioni. In questo modo è possibile tenere in considerazione buona parte delle fonti di rischio.

È bene tenere a mente che i fattori CIA sintetizzano egregiamente il risultato ottimale che si dovrebbe ottenere sull'informazione gestita. Tuttavia, il processo che porta alla mitigazione del rischio cibernetico è tanto più efficace quanto più si è in grado di procedere in maniera deterministica e di parametrizzare ciò che per sua natura è mutevole: il comportamento umano e la nascita di nuove vulnerabilità.

Pertanto, l'attività di *risk assessment*, la successiva fase di scostamento dal *desired state* e la mitigazione del rischio assicurano i medesimi risultati in tempi successivi solamente a parità di condizioni. Inoltre, se le modalità operative di esecuzione sono ben impostate e se gli

strumenti di supporto al processo sono regolati per garantire uniformità durante le varie fasi di analisi, si potrà considerare i risultati come consistenti nel tempo.

Tutto ciò che non è deterministico introduce incertezza, come l'attività di un hacker che sfrutta una vulnerabilità non nota o un errore umano a cui il sistema non è preparato a rispondere. Ma questo grado di incertezza, se il processo di mitigazione del rischio è stato ben eseguito, dovrebbe rientrare nella casistica del c.d. rischio residuale.

I reati informatici sono certamente causa di enormi danni ai singoli o alle organizzazioni, ma sono conseguenti ad un'azione attiva, commessa attraverso strumenti diretti o indiretti da parte di criminali informatici. Grazie alla comprensione dei fattori CIA è possibile includere nel rischio cibernetico detti strumenti, in particolare quelli indiretti, ovvero tutti gli elementi "passivi". Questi elementi sono quelli derivanti dall'impostazione del sistema di sicurezza informatica, tenuto conto della specificità di quest'ultimo.

Fattori attivi e passivi dovrebbero essere entrambi previsti da un'attività di valutazione del rischio ben impostata. Infatti, il *risk assessment* ha come suo elemento chiave, iniziale, la definizione del contesto e dell'ambito in cui viene eseguito. Ovviamente la preparazione e l'esperienza del personale che esegue tale attività ha un impatto significativo sul risultato. Inoltre, un'attività di valutazione del rischio ben articolata prevede tre fasi: identificazione del rischio, analisi del rischio e ponderazione del rischio tramite degli strumenti specifici per la realtà cui si applicano.

Nella prima fase vengono identificati i rischi concernenti la sicurezza delle informazioni nel loro complesso. Proprio in questa fase si identificano gli elementi caratteristici che compongono le minacce cibernetiche, cioè del sistema informatico e del contesto cui si riferiscono. Infatti, il *cyber risk* è identificato sia dalla minaccia di generare un danno alla risorsa informatica (spesso definita come *asset*), sia dal livello di vulnerabilità di quest'ultima, cioè dalla possibilità che possa essere sfruttata da parte di terzi a danno del singolo o dell'organizzazione. Ne deriva che è impossibile impostare correttamente un sistema di sicurezza delle informazioni se non si ha contezza delle risorse gestite e della loro importanza.

Proprio per questo motivo viene eseguito il c.d. *asset inventory,* ovvero il momento in cui si identificano proprio gli asset di riferimento, catalogandoli in base al loro ruolo e utilità nella sicurezza del sistema infor-

matico, compresa l'attribuzione di responsabilità da parte dei soggetti che li gestiscono. Questo perché l'identificazione delle informazioni e degli *asset* specifici da proteggere è da attribuire a chi gestisce tali informazioni, tipicamente i responsabili dei processi o delle strutture aziendali. In questo modo, può emergere sia il valore della sicurezza delle informazioni gestite in termini di riservatezza, integrità e disponibilità, sia la gravità e il danno nel caso in cui si concretizzi un incidente informatico.

Come accennato precedentemente, il danno informatico, anche noto come *data breach* può derivare sia da fattori umani sia da fattori tecnologici. Alla prima categoria sono riconducibili i criminali informatici, cioè coloro i quali cercano un tornaconto personale o provocano un danno deliberato ai danni della vittima, oppure il personale impreparato, che commette errori o azioni in maniera inconsapevole, ma che provocano ugualmente danni in termini di sicurezza delle informazioni. Nel secondo caso, ci si riferisce alle risorse informatiche coinvolte nella gestione delle informazioni, che possono danneggiarsi a causa di eventi naturali, di incidenti involontari, o diventare obsolete oppure essere mal configurate.

Per quanto riguarda la seconda fase, quella di analisi del rischio, viene effettuato il calcolo moltiplicando la probabilità per l'impatto relativo ai diversi eventi indesiderati possibili. Una valutazione a tutti gli effetti delle possibili conseguenze che risulterebbero nel caso le minacce si concretizzassero. Ciò è reso possibile mediante metodi qualitativi, cioè riferiti a scale di valutazione, e quantitativi, stimando opportunamente la probabilità che la minaccia si concretizzi. Proprio per questo motivo è necessario il coinvolgimento delle persone che gestiscono gli asset nel perimetro di analisi. Anche in questo caso, l'esperienza del personale coinvolto nell'eseguire tale attività ha un impatto significativo sul risultato dell'analisi.

Infine, nella terza ed ultima fase, quella di ponderazione del rischio, sono stabiliti i criteri di accettazione del rischio, ovvero i valori di riferimento rispetto ai quali saranno attuate le azioni di mitigazione del rischio. Tra questi criteri, a titolo esemplificativo, vi sono i vincoli di budget, determinati fattori organizzativi o tecnologici, vincoli temporali, legali o contrattuali. Considerando i suddetti valori, l'individuo o l'organizzazione procede con la classificazione dei rischi in base alla loro priorità, ovvero in base al livello più elevato di rischio e quindi definendo quale di essi non sia possibile considerare come accettabile.

Pagine omesse dall'anteprima del volume

PARTE II
TESTIMONIANZE

Di seguito riportiamo gli autori che hanno contribuito
alla PARTE II – Testimonianze

Sebastian Zdrojewski, titolare della società "Rights Chain" la cui mission è la gestione e protezione della proprietà intellettuale e delle informazioni digitali. CTO in diverse realtà, da piccoli ISP a System Integrator. Professionista ICT.

Roberto Foschi, Cyber Security Risk Manager, responsabile della Sicurezza delle Informazioni presso TELECO (PMI Innovativa iscritta MISE), Program/Project Manager PMP® PMI Certified. Negli ultimi anni ha supportato con AgID (Agenzia per l'Italia Digitale) molte P.A. Centrali e Locali nel Cyber Risk Assessment e Management di diverse Infrastrutture Critiche.

Federica D'Annibale, Attualmente impegnata in Dedalo GRC advisory, società di consulenza specializzata nella Governance dei Sistemi Informativi, è consulente in ambito IT & Security Governance, Risk Management e Compliance con esperienze nel settore pubblico e privato. Certificata ISO/IEC 27001 Auditor e ITIL 4 Foundation.

Antonio Broi, Sottufficiale del Corpo della Guardia di Finanza (qualificato CFDA Computer Forensic & Data Analysis) – svolge nel suo free-time attività di sviluppo software pubblicando nella distro Tsurugi-linux.org e formazione nella Onlus lab4int.org APS dirette a Law Enforcement.

Costanza Matteuzzi, Avvocato del Foro di Firenze. Membro di Tsurugi Linux, progetto open source DFIR. Esperta di criminalità informatica di cui si occupa a livello giudiziale e stragiudiziale. Esperta di tutela della protezione dei dati e cyber security. Consigliere della Associazione Women4cyber, Capitolo Italiano. Membro di FBA LAB, Associazione che si occupa di scienze forensi.

Premessa: Genesi di un conflitto

di Giovanni Battista Caria

Il primo vero conflitto digitale possiamo ricordarlo nelle guerre hacker degli anni 80, dove scontri digitali ebbero ripercussioni reali nella vita americana.

Seppur diverso lo possiamo definire il primo vero e proprio conflitto su vasta scala.

Oggi il conflitto Russia-Ucraina pone uno stravolgimento della vita digitale. Gli attacchi si ripercuotono in maniera netta sulla vita di ogni giorno e i dati dei cittadini (sia russi che ucraini) sono in balia di migliaia di persone e non proprio con buone intenzioni.

Questo conflitto, al di là delle motivazioni, non ha limiti di sorta e una forma di anarchia digitale va a toccare, purtroppo, anche gli innocenti.

Altro aspetto importante è che non solo gli hacktivisti e coloro che sono realmente motivati si schierano da una parte o dall'altra, ma intervengono anche l'intelligence e criminali di ogni ambito, che con la scusa di "aiutare" non fanno altro che eseguire colpi specifici, raccogliere informazioni e continuare la loro scalata criminale.

Su questi ultimi fatti nessuna legislazione è realmente pronta, il conflitto digitale ha preso tutti di sprovvista.

La mancata previsione è un forte gap di ogni governo e sarà sicuramente necessario prendere in considerazione anche questi aspetti nel prossimo futuro, specialmente rispetto alle infrastrutture critiche. Se c'è una cosa che dobbiamo imparare da questo conflitto è che basta la volontà per bloccare un servizio e le difese fino ad ora pensate non sono sufficienti.

Ma torniamo alla genesi.

Ogni specialista in intelligence aveva già fiutato qualcosa, determinati attacchi erano focalizzati su determinati target e provenivano sempre dagli stessi luoghi.

Era palese che dietro vi fosse un piano ben preciso: prove generali o necessità di valutare e raccogliere informazioni?

In questa parte parleremo di quanto succede realmente durante il conflitto, di alcuni aspetti poco conosciuti e di retroscena interessanti da parte di chi vive il conflitto direttamente.

Internet: morta per le troppe ferite (autoinflitte)

di Sebastian Zdrojewski

Correva l'anno 2001, era così che si apriva la seconda edizione di *"Hacking Exposed"*, forse uno dei libri più importanti di quel periodo in materia di sicurezza informatica. Una bibbia in cui venivano descritte tecniche base per portare avanti attacchi informatici con un solo scopo: quello di aiutare gli esperti a prevenirli.

Era un periodo di grande innovazione, il pieno della bolla ".com". Yahoo! era il portale più importante al mondo, i social media come li conosciamo oggi non esistevano. Non c'erano smartphone, il Nokia 3310 era lo strumento di comunicazione perfetto (oltre che indistruttibile). Erano gli anni in cui, per diletto e per evangelizzare il concetto di sicurezza informatica, si girava allo SMAU (la fiera di riferimento all'epoca per l'informatica e l'innovazione) accedendo alle primissime reti *wi-fi* [1], tutte rigorosamente configurate con credenziali di default sia per gli SSID che per gli apparati. E si cambiavano le password con credenziali che non fossero quelle di fabbrica. Già all'epoca il marketing spingeva per mostrare le potenzialità del prodotto: noialtri si cercava di dimostrare le problematiche.

Già all'epoca Internet non era un luogo sicuro. I "worm" (software maliziosi che si propagavano in rete autonomamente al fine di trovare sistemi vulnerabili) già erano in circolazione da tempo. Partendo dal progenitore più famoso "ILOVEYOU" [2] che ha infettato con successo dieci milioni di sistemi nel 2000 con un banale allegato, passando da Code Red [3] che infetta quasi mezzo milione di sistemi con Microsoft IIS a sua volta superato pochi mesi dopo da Nimda [4] associato, stavolta, a niente meno che Al Quaeda, poi associato al governo cinese. Blaster [5] che nel 2003 che si propagava nelle reti Microsoft Windows mettendo in ginocchio le aziende per giorni, o ancora Slammer [6] che nello stesso anno è riuscito a mettere in crisi Internet sfruttando una vulnerabilità di SQL server (con appena 376 byte di dati).

1. https://it.wikipedia.org/wiki/Wi-Fi
2. https://it.wikipedia.org/wiki/ILOVEYOU
3. https://it.wikipedia.org/wiki/Code_Red_(virus)
4. https://en.wikipedia.org/wiki/Nimda
5. https://en.wikipedia.org/wiki/Blaster_(computer_worm)
6. https://en.wikipedia.org/wiki/SQL_Slammer

Pagine omesse dall'anteprima del volume