

La sicurezza informatica per l'elettricista

Stefano Toffano

**LA SICUREZZA INFORMATICA
PER L'ELETTRICISTA**

Manuale

BOOK
SPRINT
E D I Z I O N I

www.booksprintedizioni.it

Copyright © 2023
Stefano Toffano
Tutti i diritti riservati

Indice

Prefazione	9
1. Parte teorica di una rete dati.....	15
1.1. <i>Aspetti hardware e software di una rete</i>	15
La tecnologia trasmissiva.....	15
La scala	16
Tipi di rete Wireless.....	18
Topologia	19
Software delle reti: modello ISO-OSI.....	21
1.2. <i>Rete locale</i>	22
Ethernet	22
TCP/IP	24
UDP/IP.....	24
Client – Server.....	24
Gateway.....	25
HTTP	26
HTTPS.....	26
FTP	26
IMAP	27
IP Address	27
DHCP.....	28
Comprendiamo le subnet (sotto rete).....	29
Indirizzi IP utilizzabili	30
URL	31
DNS	31
Frame Ethernet.....	32
Intranet ed Extranet	33
VLAN.....	33
Cloud	34

NAT	35
VPN	36
Wi-Fi	37
Network Tools	38
Port forwarding	40
1.3. <i>I componenti attivi di una rete dati</i>	41
Modem	42
Router	43
Firewall	45
Switch	47
Access Point.....	50
2. Comprendere la sicurezza informatica	54
2.1. <i>La sicurezza</i>	54
Vediamo i principali obiettivi della progettazione...	57
Attacco informatico.....	59
Esecuzione e codici nocivi.....	62
Malware	63
Virus.....	63
Ransomware	64
Worm	66
Trojan horse	66
RAT	67
Keylogger	68
Adware	68
Spyware	69
Rootkit	69
Logic bomb.....	70
Botnet.....	70
Antimalware	71
2.2. <i>Ingegneria sociale</i>	74
Phishing	75
Shoulder surfing.....	76
Dumper diving.....	76
Snooping.....	77

Tailgating	77
Impersonification	78
Hoax	78
Baiting.....	79
3. Valutazione dei rischi	81
3.1. <i>Generalità</i>	81
Lo scenario.....	81
L'information security.....	82
Quattro regole essenziali.....	83
Gli obiettivi della norma e quindi i nostri obiettivi	83
Contesto dell'organizzazione	84
Parti interessate	84
Leadership	85
Gli elementi costitutivi.....	85
La pianificazione	86
Analisi del rischio	86
Obbiettivi e pianificazione	86
Comunicazione.....	87
Documentazione.....	87
Pianificazione	88
Valutazione	88
Non conformità e azione correttiva	88
Miglioramento continuo	90
3.2. <i>Obbiettivi</i>	90
Politiche per la sicurezza delle informazioni.....	90
Organizzazione della sicurezza delle informazioni....	90
Sicurezza delle risorse umane	91
Gestione degli Asset (risorse-beni)	91
Controllo degli accessi.....	92
Sicurezza fisica e ambientale.....	93
Sicurezza delle attività operative.....	94
Sicurezza delle informazioni	94
Acquisizione sviluppo e manutenzione dei sistemi	95
Relazioni con i fornitori e/o collaboratori	95

Gestione degli incidenti relativi alla sicurezza delle informazioni	95
Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa	96
Conformità.....	96
Stimare i rischi	97
Trattare i rischi.....	97
Opzioni di trattamento dei rischi	98
Componenti per la sicurezza applicata.....	98
4. Parte pratica di una rete dati	102
4.1. <i>Utilizzo di VLAN, sottorete tramite Router, reti Guest WLAN</i>	102
VLAN.....	102
Sottorete	104
Reti Guest WLAN	104
Dispositivi connessi.....	107
4.2. <i>Dispositivo remoto, facciamo il Port Forwarding</i> ...	112
4.3. <i>Situazione tipo di un locale aperto al pubblico</i>	116
4.4. <i>Industria 4.0</i>	117
4.5. <i>Risposta ad alcune domande che mi fanno sulla sicurezza informatica</i>	120
Gestione VPN, perché usarla? come gestirla?	120
Il DDNS ha un costo?.....	122
Perché la scelta del marchio Zyxel	123
Rischi e problemi di dispositivi smart di dubbia provenienza	126
Bisogna installare un armadio “Rack”?	126
Conclusione	129

Prefazione

Vedo sempre più spesso produttori senza scrupoli che vendono dispositivi smart a ignari installatori elettrici ed elettronici, senza dare informazioni accurate su come collegarli ad una rete dati; senza fare un minimo di formazione e soprattutto senza comprendere quali siano i rischi determinati da una scarsa conoscenza di questi aspetti.

Quello dell'elettricista, a mio parere, è uno dei mestieri più belli del mondo: si deve conoscere una moltitudine di settori, uno dei quali è proprio quello del funzionamento di una rete informatica.

Nella guida CEI 306-17 si parla distesamente di come funziona una rete informatica, il problema è che gli anni passano, le tecnologie cambiano in modo molto veloce e molti non comprendono una guida redatta in un modo accademico.

Inoltre, spesso le guide non vengono aggiornate in modo costante, adattando o cambiando il loro contenuto in base alle esigenze del momento.

Mi chiamo Stefano Toffano, esperto in sicurezza informatica, da anni studio e mi aggiorno per *rimanere al passo* con un mondo digitale tanto affascinante quanto pieno di rischi.

Da circa dieci anni mi dedico a questo settore, inoltre ho deciso anche di riprendere gli studi, al fine di accrescere le mie conoscenze e competenze nel campo. Precedentemente ero un installatore elettrico ed elettronico, specializzato

in sicurezza e domotica. Nel tempo, proprio grazie alle mie pregresse conoscenze in diversi settori, compresi l'importanza delle infrastrutture di rete, della protezione dei dati e delle informazioni del cliente, decisi di studiare da zero.

Compresi come per me e altri colleghi, molte volte si faceva per sentito dire, o perché un produttore ti diceva cosa fare, ma senza sapere se fosse corretto oppure no.

Chiaramente fu una decisione importante, in quanto dovevo investire molto tempo e denaro, consapevole che una volta cominciato, non c'è una fine degli studi, ma una costante formazione e aggiornamento, cosa che tra l'altro è indispensabile in tutti i settori lavorativi.

Il primo step fu la formazione Cisco CCNA, che mi ha aperto un mondo: cominciai a scegliere un brand che mi rispecchiasse, fu amore a prima vista, tant'è che, ad oggi, sono un partner Zyxel MSP (Managed Service Provider), con tanto di certificazioni costantemente aggiornate.

Ciò non era tuttavia sufficiente. Nonostante avessi cominciato a lavorare nel settore come sistemista di rete, mi resi conto che bisognava fare ancora molto, sia per la mia formazione, sia per la consapevolezza del mio cliente, il quale, negli anni, diventò proprio la figura dell'elettricista.

Iniziai a comprendere e dedicare più tempo alla sicurezza informatica, partendo con lo studiare le normative di settore, in questo caso la ISO/IEC 27001 e la sua famiglia 27xxx, approfondendo e certificandomi EC-Council EHA (Ethical Hacking Associate) per comprendere meglio le potenziali minacce di Internet. Attualmente ho invece iniziato la formazione per le indagini digitali forensi.

Innanzitutto, voglio motivare chi leggerà questo libro: lo si può definire una guida, oppure chiamare manuale; ad ogni modo, è per me importante sottolineare che la formazione in ambito informatico è qualcosa di fondamentale.

Vorrei, attraverso questo manuale, eliminare la convinzione che formarsi sia una perdita di tempo, che collaborare con chi è specializzato porti via clientela, perché, al contrario, la collaborazione tra esperto e installatore è fondamentale.

Proprio per questo motivo, da qualche tempo ho iniziato anche a fare formazione specifica per gli elettricisti, per poter fornire loro le conoscenze base che possano permettere un'evoluzione veloce e costante nel settore informatico e nel campo dell'installatore elettrico ed elettronico.

In questo periodo storico, l'elettricista e/o lo specialista di settore installa impianti allarme intrusione, videosorveglianza, impianti domotici, dispositivi smart... tutti connessi a Internet, con i rischi che ne derivano.

Nelle prossime pagine fornisco informazioni su come funziona una rete dati, su cosa sapere per tutelare il cliente e il nostro lavoro, per avere un'idea di cosa fare in termini estremamente pratici.

Non potrò entrare nello specifico, in quanto in ogni situazione è sempre necessario comprendere il contesto, le esigenze del cliente e molti altri fattori.

Va anche tenuto conto dell'evolversi delle nuove tecnologie, poiché quello che scrivo oggi, tra qualche tempo in alcuni casi sarà già passato, come è capitato alla guida CEI menzionata all'inizio.

Nel presente manuale si parlerà di argomenti ostici e di argomenti facili. Alcuni sono conosciuti e altri no, ma dedicando il giusto tempo all'argomentazione trattata, tutto si comprenderà in modo facile.

Ho sempre voluto evitare una formazione accademica o un apprendimento *a pappagallo*, certamente termini e sigle vanno imparati, ma più importante dal mio punto di vista è comprendere il concetto.

Prima di passare alla parte teorico-pratica del libro, vorrei soffermarmi su un pensiero che riguarda la vita digitale di ognuno di noi.

Il tema del mondo iper-connesso e dei social mi sta particolarmente a cuore, perché riguarda la vita di tutti i giorni: nel mondo e in particolare nella nostra amata Italia, la cultura informatica, di sicurezza e sui social è a dir poco vergognosa.

Moltissime persone, spinte dal desiderio di apparire, di comunicare, di rendersi importanti, mettono in rete tutto quello che fanno durante la giornata; persone che sarebbero sconosciute diventano, attraverso il mondo digitale, dei personaggi seguiti da moltissime persone o per simpatia o per quello che fanno, senza valutare il giusto e lo sbagliato.

Anche miei conoscenti pubblicano immagini delicate in cui mostrano la propria casa, la propria famiglia, i minori (anche molto piccoli), oppure fanno video e foto di feste, vacanze, auto... come se pensassero che Internet sia un mondo meraviglioso e fantastico!

La mancanza di una formazione scolastica dedicata al mondo digitale è una lacuna gravissima: si pensi a quando si vuole guidare un'auto o una moto, in questi casi bisogna avere una patente che si ottiene sostenendo esami pratici e teorici e, solo se la si ottiene, si può allora guidare un mezzo (e nonostante ciò capitano ancora molti incidenti).

Per quanto riguarda il mondo digitale, invece, oltre alla totale assenza di divieti, molti genitori lasciano in mano a giovanissimi e bambini dei dispositivi come lo smartphone, sempre connessi a Internet, ciò crea una dipendenza pericolosissima, perché non ci si rende conto dei rischi che si corrono utilizzando queste tecnologie.

Nella rete, quello che la gente vede è solo la punta dell'iceberg, mentre il sommerso è enorme: le pagine social vengono seguite, oltre che da eventuali amici, anche da ladri di informazioni, pedofili e delinquenti in genere.