

Sommario

1. Introduzione di <i>Giovanni Ziccardi</i>	pag. 9	4.1. Il quadro attuale e il cosiddetto “legal tech”	pag. 18
1.1. La gestione digitale dell'emergenza	pag. 9	4.2. Il giurista tra dati e algoritmi	pag. 19
1.2. La formazione per protegersi dagli attacchi informatici	pag. 10	4.3. La digitalizzazione delle professioni grazie al legal tech	pag. 19
1.3. Un percorso verso la sicurezza	pag. 11	4.4. Implementare il legal tech nella professione quotidiana	pag. 19
2. Le misure di sicurezza informatica e il segreto professionale di <i>Pierluigi Perri</i>	pag. 11	4.5. Il legal tech: lo stato dell'arte e le prospettive future	pag. 20
2.1. L'attenzione alla sicurezza e al segreto	pag. 11	4.6. La mappa del legal tech: orientarsi e documentarsi	pag. 21
2.2. Tre indicazioni preliminari per un'analisi del rischio	pag. 13	5. Il quadro della cybersecurity personale e professionale di <i>Giovanni Ziccardi</i>	pag. 21
2.3. Le minacce tipiche alla sicurezza	pag. 14	5.1. L'avvento del dato digitale e la sicurezza informatica nelle professioni	pag. 21
2.4. Le raccomandazioni in tema di sicurezza dello smart working e del telelavoro	pag. 15	5.2. L'importanza e la centralità del dato nelle professioni moderne	pag. 22
2.5. Le linee guida nazionali di AgID	pag. 16	5.3. La mappatura del tipo di dati trattati	pag. 22
3. Una nuova idea di smart-working professionale sicuro di <i>Giovanni Ziccardi</i>	pag. 17	5.4. Qualche esempio elementare di analisi del rischio	pag. 23
3.1. L'improvvisa necessità di lavorare da casa	pag. 17	6. Il GDPR, lo studio digitalizzato e i principi di protezione dei dati di <i>Giulia Escurolle</i>	pag. 24
4. Diritto, dati e automazione: le nuove frontiere del legal tech di <i>Silvia Martinelli</i>	pag. 18		

Sommario

6.1. La protezione dei dati nello studio professionale	pag. 24	8.1. Comprendere e utilizzare la multiutenza	pag. 35
6.2. Gli adempimenti del professionista	pag. 24	8.2. La suddivisione delle utenze	pag. 35
6.3. L'informativa e il registro dei trattamenti	pag. 25	8.3. Gli account "amministratore" e "standard"	pag. 36
6.4. L'individuazione dei soggetti	pag. 26	8.4. La sicurezza dei sistemi configurati con la multiutenza	pag. 37
6.5. La nomina del DPO	pag. 26	9. Il "peso" dei dati trattati e il "ciclo di vita" di <i>Giovanni Ziccardi</i>	pag. 37
6.6. Le misure di sicurezza	pag. 27	9.1. Comprendere la natura e il "peso" del dato	pag. 37
7. Regole, best practices e policy ai fini della protezione dei dati di <i>Giovanni Ziccardi</i>	pag. 28	9.2. Interpretare il dato come qualcosa di "vivo"	pag. 39
7.1. Un primo set di regole (per sé) o di istruzioni (per gli altri)	pag. 28	10. La corretta gestione dei profili di autenticazione e di autorizzazione di <i>Alessandra Salluce</i>	pag. 40
7.2. L'uso degli strumenti informatici e le misure adeguate di sicurezza in ambito professionale	pag. 28	10.1. L'importanza di una corretta gestione di autenticazione e autorizzazione	pag. 40
7.3. La gestione interna ed esterna di possibili data breach	pag. 30	10.2. Il concetto di autenticazione	pag. 40
7.4. La protezione dagli attacchi di phishing	pag. 32	10.3. La corretta gestione della password	pag. 41
7.5. Usare le policy per stabilire regole chiare per la sicurezza	pag. 33	10.4. Il concetto di autorizzazione (e la sua importanza)	pag. 42
8. L'importanza centrale della multiutenza di <i>Alessandra Salluce</i>	pag. 35	10.5. Gli attacchi più comuni ai sistemi di autenticazione e autorizzazione	pag. 42

Sommario

11. I profili di sicurezza nella procedura di autenticazione di <i>Alessandra Salluce</i>	pag. 44	16.1. La centralità del backup	pag. 54
11.1. Autenticazione informatica e profili di sicurezza	pag. 44	16.2. Il backup: caratteristiche essenziali	pag. 55
11.2. "Qualcosa che si conosce"	pag. 44	16.3. I sistemi di backup "zero-knowledge"	pag. 56
11.3. "Qualcosa che si possiede"	pag. 44	17. I problemi giuridici e di sicurezza correlati all'installazione e utilizzo di software non riferito alle attività lavorative di <i>Chiara Ciccio Romito</i>	pag. 57
11.4. "Qualcosa che si è"	pag. 45	17.1. Un'introduzione al problema pratico	pag. 57
12. L'aggiornamento dei sistemi operativi e le patch dei software come strumenti di sicurezza di <i>Alessandra Salluce</i>	pag. 45	17.2. Definizione di software	pag. 57
12.1. Il computer sicuro e aggiornato	pag. 45	17.3. L'uso lecito del software	pag. 57
13. Il tracking delle informazioni di <i>Giovanni Ziccardi</i>	pag. 48	17.4. Gli aspetti di cybersecurity	pag. 58
14. Gli antivirus e i firewall di <i>Alessandra Salluce</i>	pag. 49	17.5. Il GDPR e gli obblighi di accountability	pag. 59
14.1. Gli antivirus	pag. 49	17.6. Un esempio di policy per la corretta gestione del software	pag. 59
14.2. I firewall	pag. 51	18. La cifratura dei dati del professionista di <i>Gabriele Suffia</i>	pag. 61
15. La "filosofia" quotidiana della ridondanza del dato di <i>Giovanni Ziccardi</i>	pag. 52	18.1. Le problematiche pratiche	pag. 61
15.1. L'importanza di avere il dato in più "luoghi"	pag. 52	18.2. Dall'origine della crittografia al suo utilizzo oggi	pag. 61
16. Il backup e il ripristino del sistema di <i>Alessandra Salluce</i>	pag. 54	18.3. La cifratura dei dati sul dispositivo	pag. 62

Sommario

18.4. Le comunicazioni cifrate	pag. 63	22.1. Il phishing come minaccia primaria nel quadro odierno	pag. 70
18.5. Un esempio di policy di gestione	pag. 64	22.2. Phishing, spear phishing e whaling	pag. 70
18.6. La cifratura dei dati e il diritto	pag. 65	22.3. Tipologie di phishing attack	pag. 71
19. Prendere confidenza con la crittografia di <i>Giovanni Ziccardi</i>	pag. 66	22.4. Disciplina giuridica	pag. 73
19.1. L'importanza di oscurare i dati	pag. 66	22.5. Anti-phishing policy	pag. 73
20. La navigazione sicura e anonima di <i>Gabriele Suffia</i>	pag. 67	23. Alzare il proprio livello di protezione dai virus di <i>Giovanni Ziccardi</i>	pag. 75
20.1. Un cenno ulteriore ai firewall	pag. 67	23.1. La minaccia del malware	pag. 75
20.2. Le Virtual Private Network (VPN)	pag. 67	24. La protezione dal ransomware di <i>Andrea Scirpa</i>	pag. 76
20.3. I proxy	pag. 68	24.1. Alcune premesse essenziali	pag. 76
20.4. Tor	pag. 68	24.2. Il ransomware	pag. 76
20.5. Browser e motori di ricerca	pag. 68	24.3. La protezione dal ransomware	pag. 77
21. Abituarsi all'uso di macchine virtuali e di portable app di <i>Giovanni Ziccardi</i>	pag. 69	24.4. Estorsione, sextortion e truffe sentimentali	pag. 78
21.1. Usare le macchine virtuali per creare ambienti sicuri	pag. 69	24.5. Protezione dalle estorsioni, sextortion e truffe sentimentali	pag. 80
22. La protezione dal phishing di <i>Samanta Stanco</i>	pag. 70	25. La vulnerabilità dei comportamenti umani di <i>Giovanni Ziccardi</i>	pag. 80

Sommario

25.1. L'importanza dei comportamenti umani in un'ottica di cybersecurity	pag. 80	26.5. Zoom Cloud Meetings	pag. 84
26. Delocalizzare e dematerializzare le riunioni e gli incontri professionali di <i>Andrea Scirpa e Samanta Stanco</i>	pag. 82	27. Cultura e migliori pratiche di <i>Giovanni Ziccardi</i>	pag. 85
26.1. Il boom dei software per videoconferenze, meeting e didattica a distanza	pag. 82	27.1. Le migliori pratiche da seguire	pag. 85
26.2. L'intervento del Garante per la protezione dei dati personali italiano	pag. 82	27.2. Conoscenza e formazione continua	pag. 86
26.3. GoToMeeting	pag. 83	28. La sicurezza dei dati presenti su smartphone e tablet di <i>Giovanni Ziccardi</i>	pag. 88
26.4. L'uso di Microsoft Teams	pag. 83	28.1. Lo studio professionale in un iPhone o in un iPad	pag. 88
		28.2. La sicurezza dello smartphone	pag. 89

Sommario

L'AUTORE

Giovanni Ziccardi, Professore di informatica giuridica, Università degli Studi di Milano

Con contributi di:

Giulia Escurole, Avvocato in Torino, Dottore di ricerca in diritto penale, Research Fellow dell'Information Society Law Center dell'Università di Milano

Silvia Martinelli, Avvocato in Milano, Assegnista di ricerca dell'Università degli Studi di Milano, Dottoranda dell'Università degli studi di Torino

Pierluigi Perri, Professore di informatica giuridica e Avvocato in Milano

Chiara Ciccia Romito, Avvocato in Modena, Research Fellow dell'Information Society Law Center dell'Università degli Studi di Milano

Alessandra Salluce, Assegnista di ricerca presso l'Università degli Studi di Milano

Andrea Scirpa, Assegnista di ricerca in informatica giuridica presso l'Università degli Studi di Milano e Research Fellow dell'Information Society Law Center

Samanta Stanco, Research Fellow dell'Information Society Law Center dell'Università degli Studi di Milano

Gabriele Suffia, Assegnista di ricerca in informatica giuridica presso l'Università degli Studi di Milano, Research Fellow dell'Information Society Law Center