

CYBERSÉCURITÉ

Patrick Lallement

Définitions

Concepts

Métiers

A detailed illustration of a metallic padlock with a silver handle, positioned on a dark, reflective surface. The background is a vibrant, abstract digital space with glowing blue and purple lines, suggesting a network or data flow. The padlock is the central focus, symbolizing security in the digital realm.

ellipses

Table des matières



1	Qu'est-ce que le cyber-espace ?	9
1.1	Les convergences	9
1.1.1	Évolution des architectures	9
1.1.2	Vers le tout numérique	10
1.1.3	Le multimédia	10
1.2	Les technologies de l'internet	10
1.2.1	Le réseau	10
1.2.2	L'adressage	12
1.2.3	Le protocole de transport	14
1.2.4	IP et la sécurité	15
1.2.5	Le pare-feu	15
1.3	Services de l'internet	17
1.3.1	Le web	17
1.3.2	Système DNS	18
1.3.3	Le web caché (<i>dark web</i>)	19
1.3.4	DNS et la sécurité	20
1.4	Le système d'information (SI)	21
1.4.1	Les fonctions du SI	21
1.4.2	Les processus	22
1.4.3	Du web 1.0 au web 2.0	24
1.4.4	Dimension importante du SI : l'être humain	25
1.4.5	Où on (re)parle d'intelligence artificielle	26
1.4.6	Éléments d'infrastructure	26
1.4.7	Configuration de base d'un poste de travail	29
1.4.8	Virtualisation	29
1.4.9	Le cloud computing	31
1.4.10	Aspects sécurité	33
1.5	Les systèmes cyber-physiques	33
1.5.1	Couplage physique/ logique	33
1.5.2	Les systèmes cyber-physiques	34
1.5.3	Les objets connectés	36
1.6	Un univers de données	40
1.6.1	Donnée/ Information	40
1.6.2	Les fichiers	40
1.6.3	Les données personnelles	42

1.6.4	Les méta-données	43
1.6.5	Le big data	44
1.7	Vers le cyber-espace	44
1.7.1	Aspects géopolitiques	44
1.7.2	Notion de puissance	45
1.8	Conclusion	45
1.9	Exercices	45
2	L'espace des risques	49
2.1	Qu'est-ce que le risque?	49
2.1.1	Définition	49
2.1.2	Évaluation	49
2.1.3	Sûreté de fonctionnement	50
2.2	Qu'est-ce que le cyber-risque?	51
2.2.1	Risque <i>vs</i> cyber-risque	51
2.2.2	Typologie du risque "cyber"	51
2.2.3	Risque sur les données	52
2.2.4	Critères DICP	52
2.2.5	Risque sur le système	54
2.2.6	Risque "sûreté" (<i>safety</i>)	54
2.2.7	Malveillance : de la menace aux dommages	54
2.2.8	Termes clés	56
2.3	Caractérisation du danger	56
2.3.1	La menace	56
2.3.2	Attaque	59
2.3.3	Vecteur d'attaque	59
2.3.4	Scénarios d'attaque	60
2.3.5	La matrice MITRE ATT&CK	60
2.3.6	Attaques de déni de service	64
2.3.7	Le malware	67
2.3.8	Cas particulier des rançongiciels (<i>ransomware</i>)	68
2.4	Caractérisation du système	71
2.4.1	Les actifs	71
2.4.2	Vulnérabilités	71
2.4.3	Faible <i>vs</i> vulnérabilité	72
2.4.4	Exploit	73
2.4.5	Analyse de vulnérabilités	73
2.4.6	Protection	74
2.4.7	Détection	74
2.4.8	Impact	75
2.4.9	Relations entre les concepts	77
2.5	La gestion des risques	80
2.5.1	Processus	80
2.5.2	P1-Identification	80
2.5.3	P2-Estimation	80
2.5.4	P3-Évaluation	81
2.5.5	P4-Traitement	82

2.5.6	Norme ISO 27005	82
2.5.7	Méthodes d'analyse de risques	83
2.6	Autres définitions	85
2.6.1	Cybersécurité	85
2.6.2	Sécurité des systèmes d'information	85
2.6.3	Lutte contre la cyber-criminalité	85
2.6.4	Cyber-défense	86
2.6.5	Cyber-guerre	86
2.7	La réponse à incident	87
2.7.1	Quelques définitions	87
2.7.2	Les incidents de sécurité	88
2.7.3	La procédure de traitement des incidents	89
2.7.4	Éléments de procédure	90
2.7.5	L'équipe de réponse à incident	93
2.7.6	Le processus de traitement	97
2.7.7	Le SIEM (<i>Security Information and Event Management</i>)	108
2.8	Les services de réponse à incident	110
2.8.1	Les CERT (ou CSIRT)	110
2.8.2	Les SOC	111
2.8.3	Différences entre CERT et SOC	111
2.9	Exercices	111
3	L'espace de confiance	121
3.1	Les lois	122
3.1.1	Évolution des lois	122
3.1.2	Loi informatique et libertés	124
3.1.3	Règlement général de la protection des données	124
3.1.4	Loi Godfrain	125
3.1.5	La cyber-criminalité dans le code pénal	125
3.1.6	Loi de confiance sur l'économie numérique - LCEN	126
3.1.7	Loi LOPSSI 2	127
3.1.8	Loi de programmation militaire - LPM	127
3.2	Les obligations légales	128
3.2.1	Conservation des données de connexion	128
3.2.2	Utilisation de la cryptographie	129
3.2.3	Cas du <i>cloud computing</i>	130
3.2.4	Les opérateurs d'importance vitale (OIV)	130
3.2.5	Les établissements financiers	131
3.2.6	La directive européenne NIS	132
3.2.7	Politique de sécurité du système d'information (PSSI)	133
3.2.8	Charte informatique au sein de l'entreprise	133
3.2.9	Les normes ISO	136
3.3	Les institutions	137
3.3.1	Agence nationale de la sécurité des systèmes d'information	137
3.3.2	Commission nationale de l'informatique et des libertés	137
3.3.3	Sous-direction de lutte contre la cybercriminalité	137
3.3.4	Brigade de lutte contre la cybercriminalité	138

3.3.5	La gendarmerie nationale	138
3.3.6	Direction générale de la sécurité intérieure	139
3.3.7	Traitement du renseignement et action contre les circuits financiers clandestins	139
3.3.8	Cyber-douanes	140
3.3.9	Les officiers de police judiciaire	140
3.3.10	La magistrature	141
3.4	Les associations	141
3.4.1	Le Clusif	141
3.4.2	Le CESIN	142
3.4.3	Le CeCyF	142
3.4.4	Signal Spam	142
3.4.5	CyberLex	142
3.4.6	Les pôles de compétitivité	142
3.5	Les métiers de la cybersécurité	143
3.5.1	La gestion de la sécurité et le pilotage des projets	143
3.5.2	Conception et maintien d'un SI sécurisé	144
3.5.3	Gestion des incidents et des crises	145
3.5.4	Le conseil	146
3.5.5	L'enseignement et la recherche	147
3.6	Exercices	148
Conclusion		153
Correction des exercices		155
3.7	Partie 1	155
3.8	Partie 2	158
3.9	Partie 3	163
Bibliographie		167