TWIST
Conseil en gestion de crise et culture du risque

twist-conseil.fr
benoit@scopic.fr • 06 32 89 01 81

CHECKLIST OPÉRATIONNELLE

Crise cyber : 25 actions des premières heures

TWIST-CHECKLIST-CYBER-V2
Référence interne · à imprimer ou afficher en cellule

À activer dès qualification d'un incident cyber : ransomware, fuite de données, intrusion SI. Cocher au fur et à mesure, horodater, no

	ACTION	HEURE	QUI	FAIT
1	**ISOLER**			H+0 H+15 min
☐	Identifier les systèmes compromis (SOC, EDR, alertes utilisateurs)			☐
☐	Déconnecter du réseau, NE PAS éteindre brutalement (perte preuves RAM)			☐
☐	Documenter l'horodatage précis de l'isolement			☐
2	**ACTIVER LES 2 CELLULES**			H+15 min H+1 h
☐	Convoquer cellule cyber technique : RSSI, SOC, prestataire IR			☐
☐	Convoquer cellule de crise générale : DG, com, juridique, RH, métier			☐
☐	Désigner un coordinateur de pont entre les 2 cellules			☐
☐	Ouvrir une main courante horodatée (qui décide quoi, quand)			☐
3	**PRÉSERVER LES PREUVES**			H+1 h H+2 h
☐	Capture mémoire (RAM dump) des machines impactées			☐
☐	Image disque forensique des systèmes compromis			☐
☐	Export logs SIEM, EDR, firewall, AD, mail + traces réseau (PCAP)			☐
4	**NOTIFIER LES AUTORITÉS**		H+24 h à H+72 h selon obligation	
☐	CNIL sous 72 h si données personnelles touchées (RGPD)			☐
☐	CERT-FR : alerte précoce 24 h + notification 72 h (NIS2)			☐
☐	ANSSI si OIV ou OSE (Loi de programmation militaire)			☐
☐	Autorité sectorielle (ARS, ACPR…) + assureur cyber			☐
5	**CADRER LA COMMUNICATION**			H+2 h H+24 h
☐	Message interne avant toute fuite externe (tous salariés)			☐
☐	Désigner UN porte-parole unique, préparer message holding			☐
☐	Anticiper FAQ médias par war-gaming express avec DG + com			☐
6	**MOBILISER UN CABINET IR**			H+1 h H+4 h
☐	Activer la préconvention IR si elle existe, sinon urgence			☐
☐	Contractualiser NDA + lettre de mission avant accès SI			☐
☐	Briefer le cabinet : périmètre, accès, contacts, horodatage			☐
☐	Établir cadence de reporting (toutes les 2 h en aigu, puis 4 h)			☐
7	**PRÉPARER REPRISE + RETEX**			H+4 h H+72 h
☐	Lister les systèmes à redémarrer en priorité (RTO/RPO)			☐
☐	Vérifier propreté avant chaque redémarrage (durcissement, IOC)			☐
☐	Désigner référent RETEX, collecter chronologie au fil de l'eau			☐
☐	Briefer parties prenantes externes (clients, partenaires, tutelles)			☐

BESOIN D'UN ACCOMPAGNEMENT ?

Contactez-nous

Premier rendez-vous téléphonique sans engagement. NDA signé dès le lancement de la mission.

06 32 89 01 81
benoit@scopic.fr
twist-conseil.fr/crise-cyber/