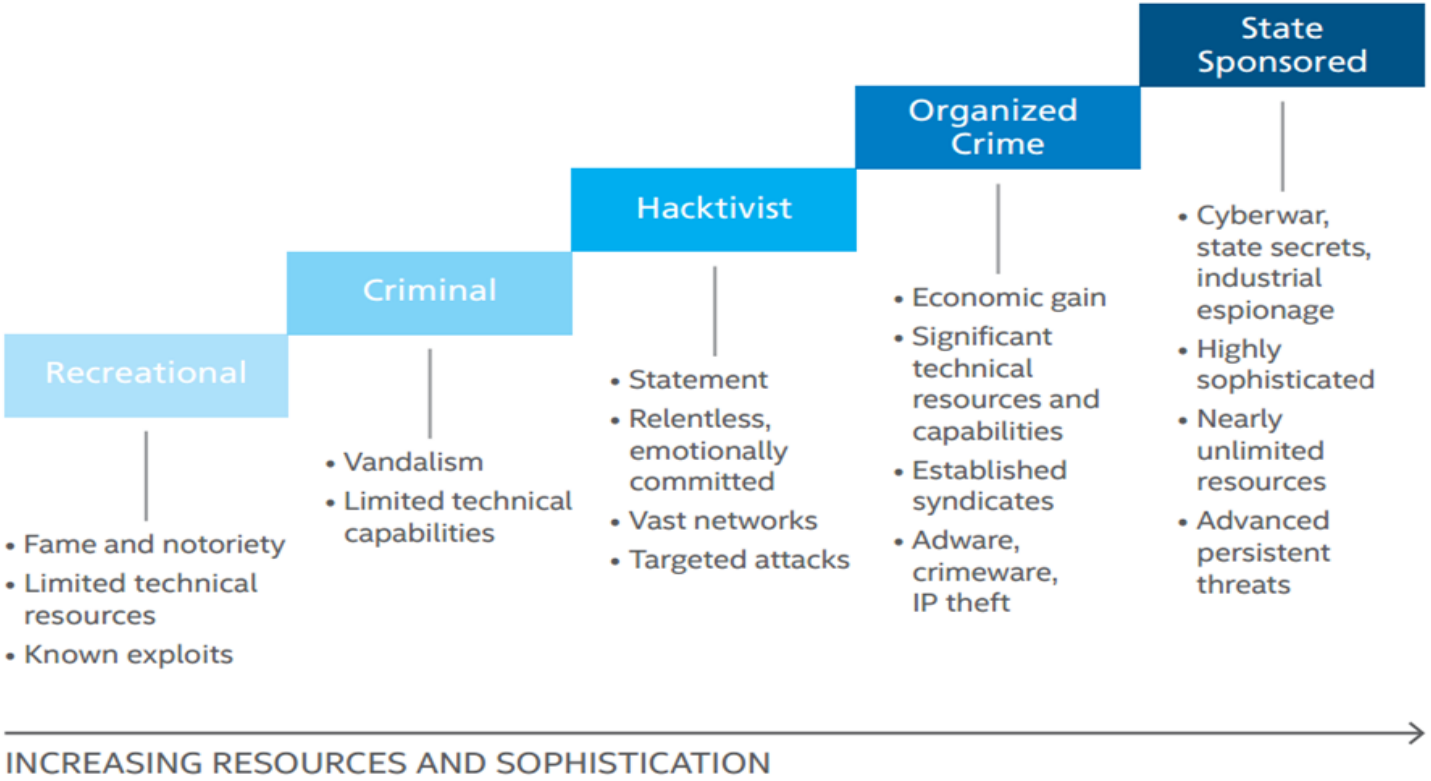
Séance d'information UCV du 18 novembre

GESTION DE CRISE ET RÉPONSES EN CAS DE CYBERATTAQUE

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Classification : Interne DGNSI
TLP:AMBER
(https://www.first.org/tlp/)

Les attaquants…



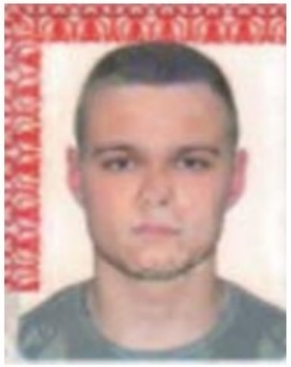
Source : Security Intelligence IBM

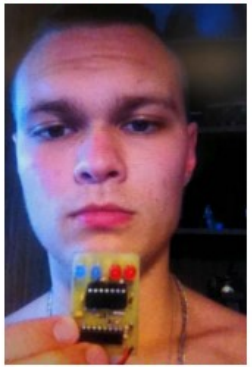
Source: https://krebsonsecurity.com/

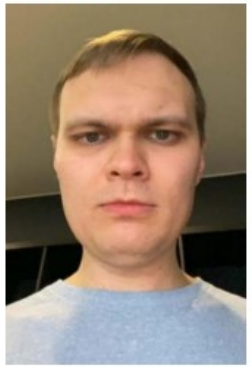
WANTED BY THE FBI

YEVGYENIY IGORYEVICH POLYANIN

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Conspiracy to Commit Money Laundering







DESCRIPTION

Aliases: Yevhgyeniy Polyanin, Yevgeniy Polyanin, Yevgveniey Igorevich Polyanon, Evegnii Igorevich Polianin, Evgeniy Polyanin, Evgeniy Igorevich Polyanin, "Ik-4d4"

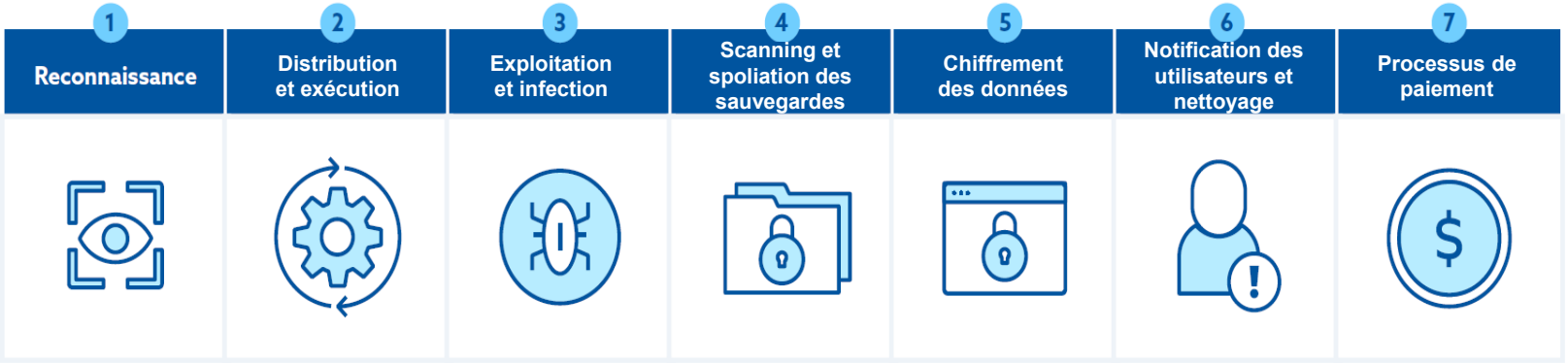
Date(s) of Birth Used: March 4, 1993	**Place of Birth:** Russia
Sex: Male	**Race:** White
Nationality: Russian	

REMARKS

Polyanin is believed to be in Russia, possibly in Barnaul, and is one of many Sodinokibi/REvil ransomware affiliates.

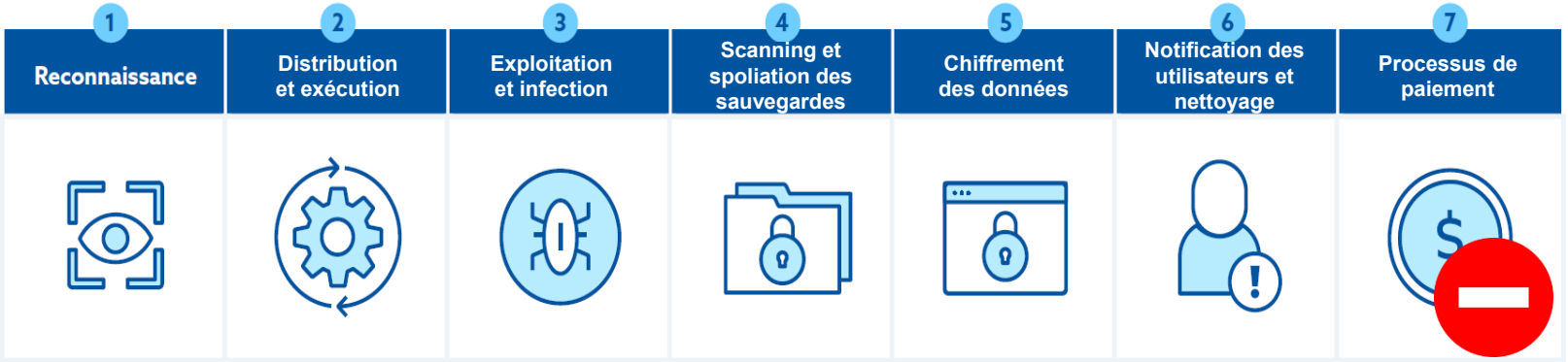
Source: https://krebsonsecurity.com/

Les 7 étapes typiques d'une cyberattaque «rançongiciel»



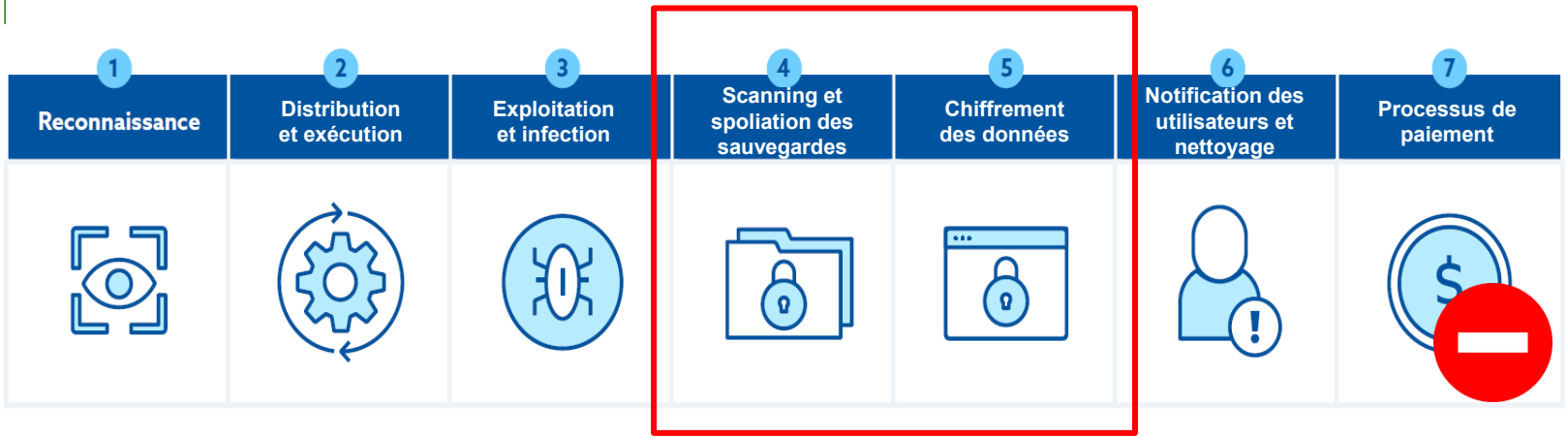
Source de l'illustration : Cloud Security Alliance (publication Ransomware in the Healthcare Cloud, 2021)

Les 7 étapes typiques d'une cyberattaque «rançongiciel»



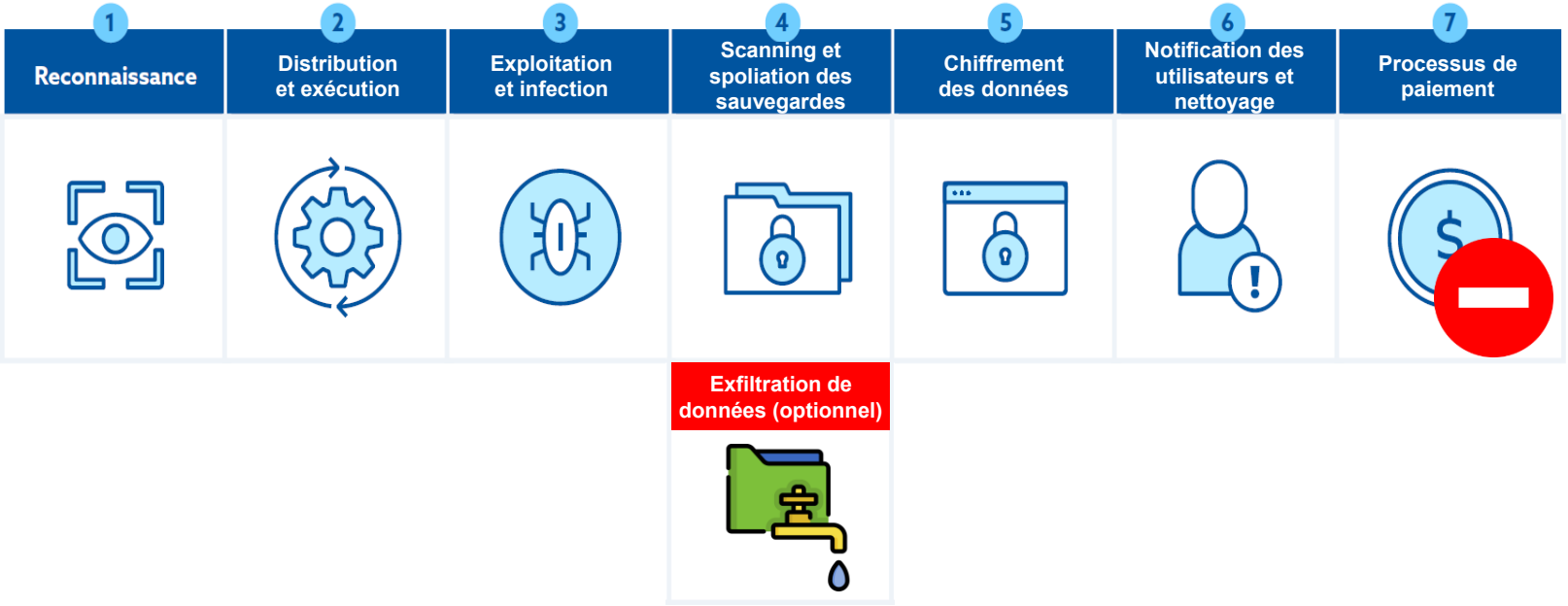
Source de l'illustration : Cloud Security Alliance (publication Ransomware in the Healthcare Cloud, 2021)

Les 7 étapes typiques d'une cyberattaque «rançongiciel»



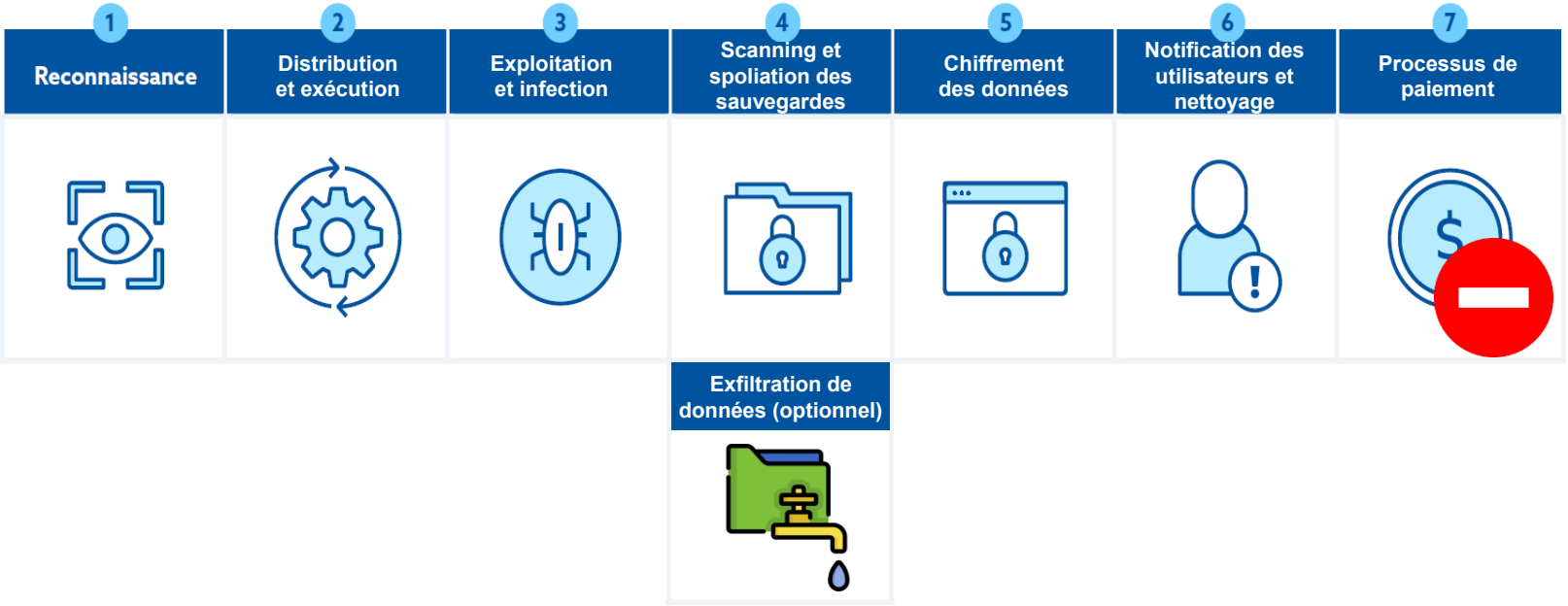
Source de l'illustration : Cloud Security Alliance (publication Ransomware in the Healthcare Cloud, 2021)

Les 7 étapes typiques d'une cyberattaque «rançongiciel»



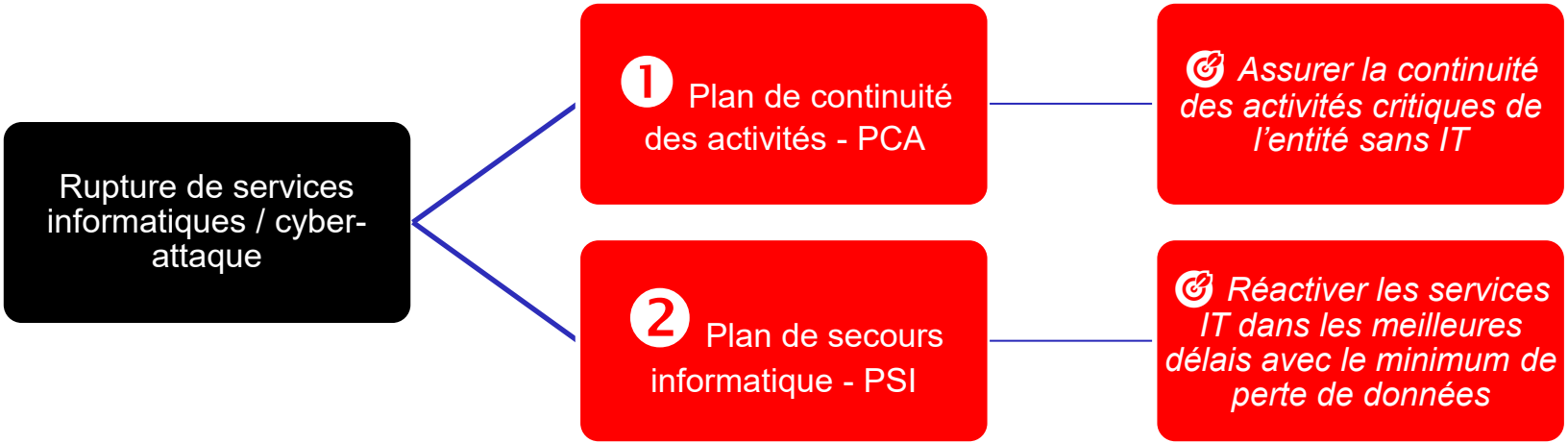
Source de l'illustration : Cloud Security Alliance (publication Ransomware in the Healthcare Cloud, 2021)

Les 7 étapes typiques d'une cyberattaque «rançongiciel»



Source de l'illustration : Cloud Security Alliance (publication Ransomware in the Healthcare Cloud, 2021)

Une réponse, 2 plans de continuité à activer et coordonner



Une réponse aux incidents qui ne s'improvise pas

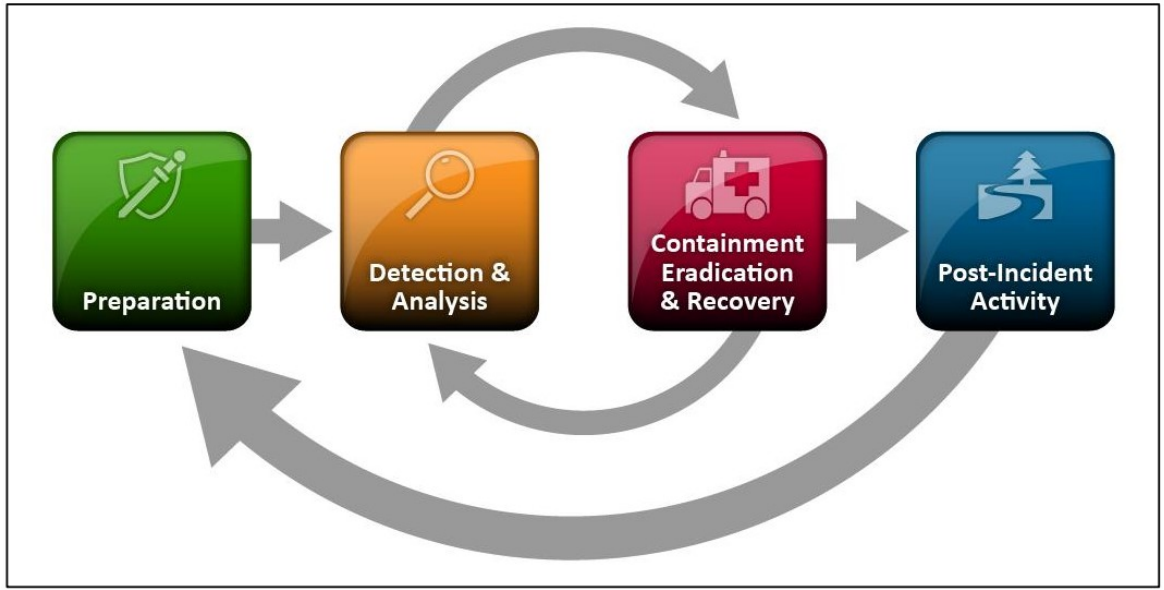


Figure 3-1. Incident Response Life Cycle

Source de l'illustration : NIST

Comment gérer la crise provoquée par une cyberattaque?

Fonctionnement normal – hors crise

Municipalité, direction de l'administration

Equipe IT

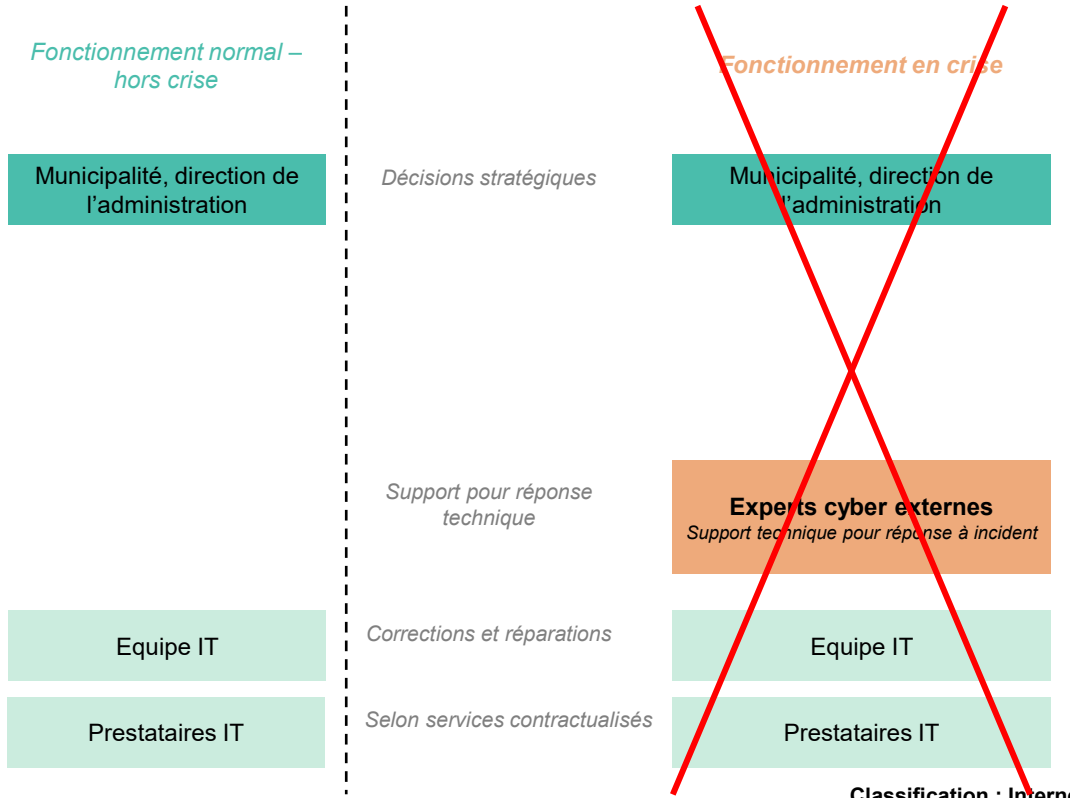
Prestataires IT

Comment gérer la crise provoquée par une cyberattaque?

Fonctionnement normal – hors crise		*Fonctionnement en crise*
Municipalité, direction de l'administration	*Décisions stratégiques*	Municipalité, direction de l'administration
	Support pour réponse technique	**Experts cyber externes** *Support technique pour réponse à incident*
Equipe IT	*Corrections et réparations*	Equipe IT
Prestataires IT	*Selon services contractualisés*	Prestataires IT

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Comment gérer la crise provoquée par une cyberattaque?



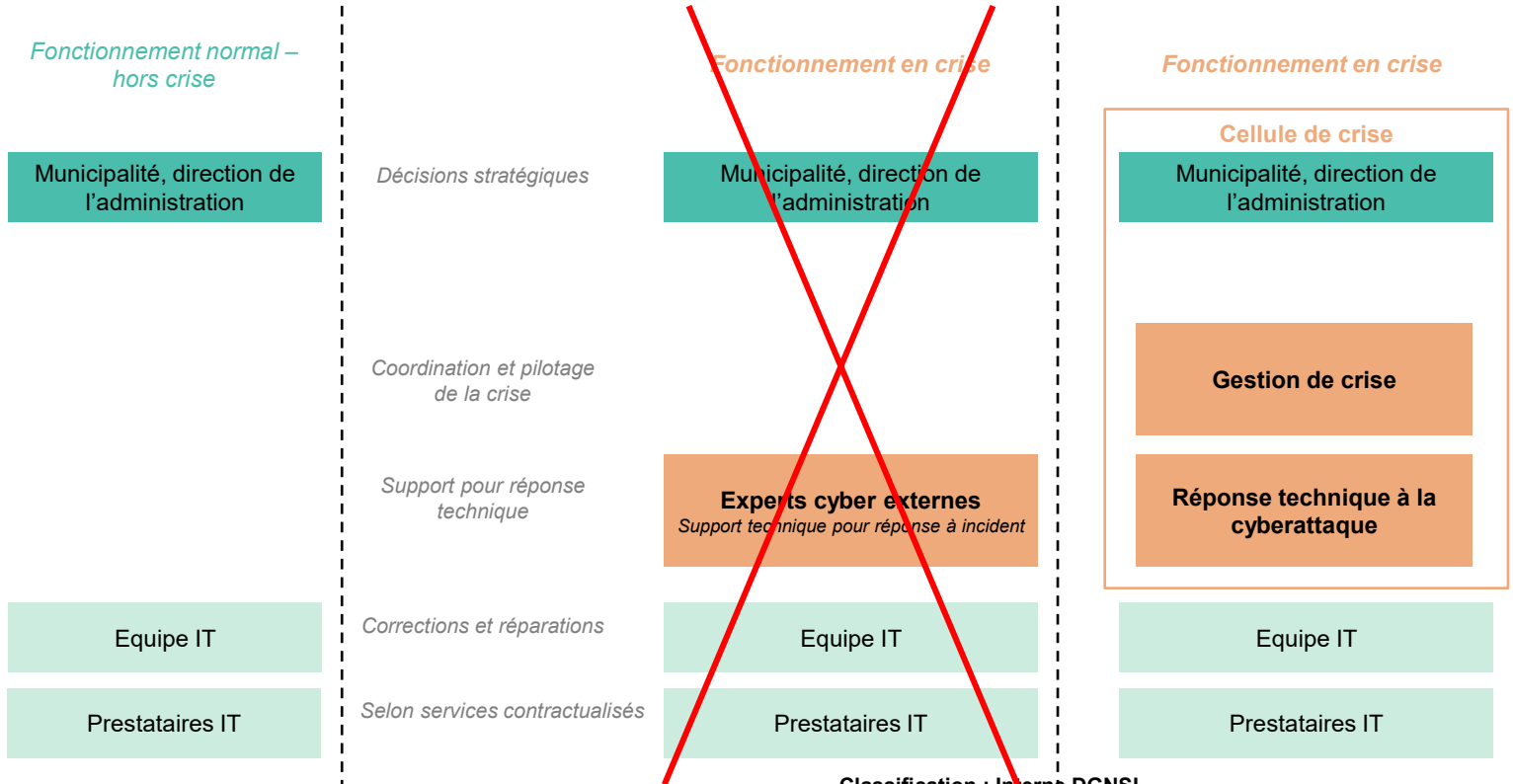
Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Classification : Interne DGNSI

TLP:AMBER

(https://www.first.org/tlp/)

Comment gérer la crise provoquée par une cyberattaque?



Comment gérer la crise provoquée par une cyberattaque?

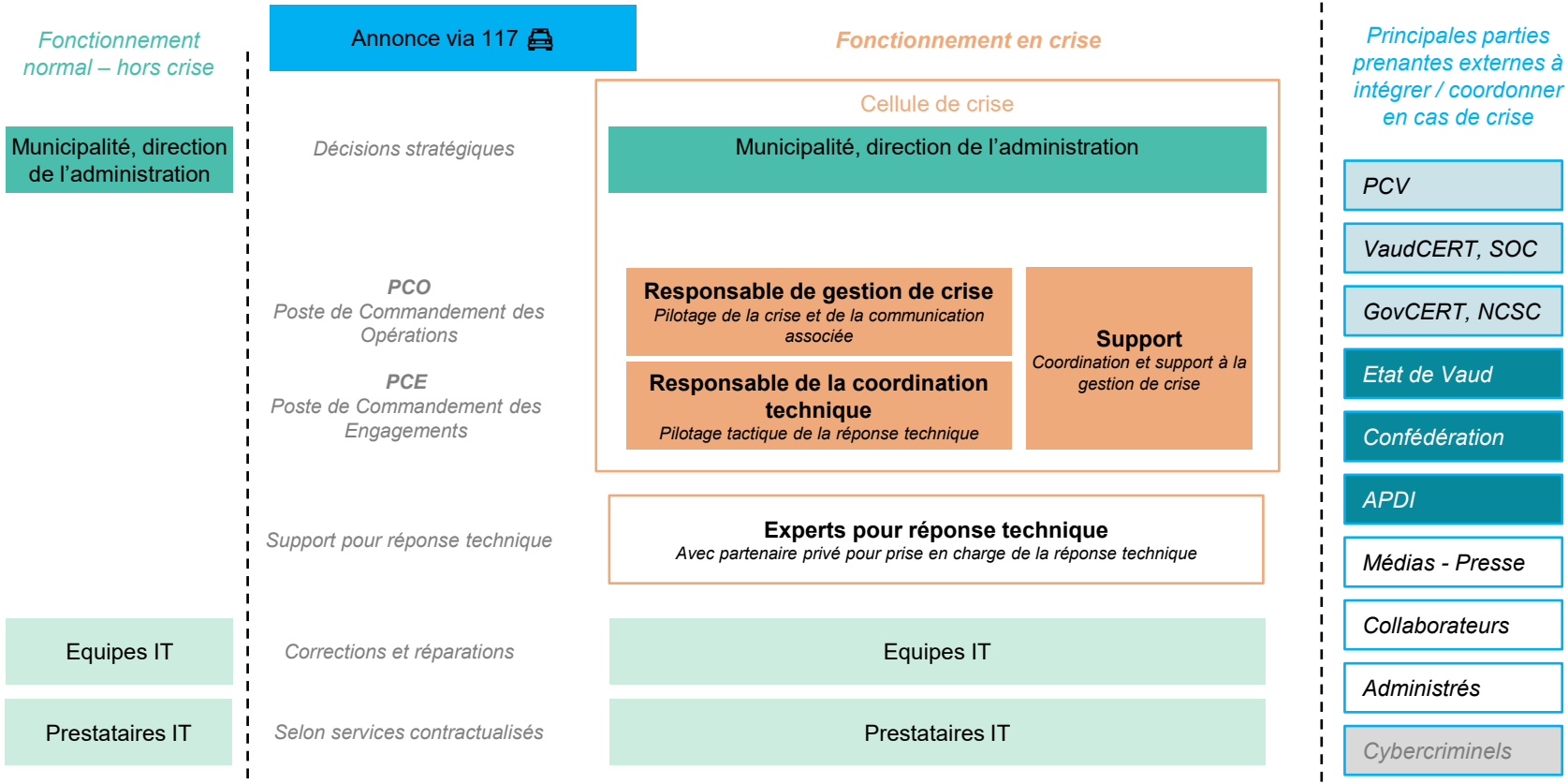
	Fonctionnement normal – hors crise	Fonctionnement en crise	Fonctionnement en crise
			Cellule de crise
Décisions stratégiques	Municipalité, direction de l'administration	Municipalité, direction de l'administration	Municipalité, direction de l'administration
Coordination et pilotage de la crise			**Gestion de crise**
Support pour réponse technique		**Experts cyber externes** *Support technique pour réponse à incident*	**Réponse technique à la cyberattaque**
Corrections et réparations	Equipe IT	Equipe IT	Equipe IT
Selon services contractualisés	Prestataires IT	Prestataires IT	Prestataires IT

Principales parties prenantes externes à intégrer / coordonner en cas de crise

- *PCV*
- *VaudCERT, SOC*
- *GovCERT, NCSC*
- *Etat de Vaud*
- *Confédération*
- *APDI*
- *Médias - Presse*
- *Collaborateurs*
- *Administrés*
- *Cybercriminels*

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Le principe d'organisation de la cellule d'urgence cantonale



Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Classification : Interne DGNSI
TLP:AMBER
(https://www.first.org/tlp/)

La communication est essentielle pour éviter une crise dans la crise

- Une communication calquée sur le rythme de conduite de la crise… et non sur l'urgence provoquée par les médias

- Des communiqués de presse et une ligne de paroles
  - Des éléments d'information précis et clairs (non techniques)
  - L'importance d'une transparence maîtrisée (timing, information non «détournable»)

- Une communication multicanale
  - En n'oubliant pas l'indisponibilité potentielle de certaines infrastructures ou informations
  - L'importance de la communication interne

- Une équipe de communication … de crise

Principales parties prenantes externes à intégrer / coordonner en cas de crise

- *PCV*
- *VaudCERT, SOC*
- *GovCERT, NCSC*
- *Etat de Vaud*
- *Confédération*
- *APDI*
- *Médias - Presse*
- *Collaborateurs*
- *Administrés*
- *Cybercriminels*

Des conseils pour <u>aussi</u> aider les communes ….

Conseils en cas de cyberattaque

Comme toute structure présente sur Internet, les communes peuvent être la cible des cybercriminels.

Les conséquences d'une attaque informatique peuvent être atténuées, à condition de prendre les bonnes mesures et d'agir vite… car, en matière de cybercriminalité, le temps joue contre nous.

Cette notice, à l'attention des communes et de leurs responsables informatiques, explique les premières actions à entreprendre en cas d'attaque par rançongiciel.

PS-SEC/202110.01

COMMENT RÉAGIR EN CAS D'ATTAQUE PAR RANÇONGICIEL

En cas de suspicion d'attaque par rançongiciel, des mesures urgentes doivent être prises :

1. **Isoler votre informatique de l'extérieur :** couper les connexions Internet, l'accès VPN ou tout autre accès distant.
2. **S'assurer que vos sauvegardes sont intègres** et les déconnecter du reste de votre infrastructure. Cela permettra de procéder à la restauration ultérieure des systèmes.
3. **Contacter la Police cantonale (117)** et demander l'entité cybercrime pour annoncer l'incident. Cette entité sera votre point de contact avec les autorités cantonales et vous aidera dans vos démarches (dépôt de plainte et première analyse), et impliquera les experts du Centre opérationnel de sécurité vaudois (SOC) en cas de nécessité.
4. **Une cellule de crise** doit être mise en place le plus rapidement possible avec, au minimum, des représentants de l'autorité communale, un responsable de la communication, un responsable informatique et une personne avec des compétences en cybersécurité.
5. **S'appuyer sur un prestataire spécialisé** en *Incident Response*, qui pourra vous aider dans la gestion technique de l'incident en cybersécurité. La collecte de preuves, via les journaux de connexions (logs) de vos équipements, sera une des premières étapes techniques effectuées afin de comprendre l'attaque et son ampleur.
6. **Annoncer l'incident auprès de la Confédération** (NCSC / GovCERT) via le site https://www.report.ncsc.admin.ch/fr/

Direction générale du numérique et des systèmes d'information (DGNSI)

Prenez en main votre sécurité informatique, utilisez ce QR code et suivez gratuitement une formation en ligne.

Pour les professionnels, rendez-vous sur : www.vd.ch/cybersecurite/

Des conseils pour <u>aussi</u> aider les communes ….

3. Contacter la Police cantonale (117) et demander l'entité cybercrime pour annoncer l'incident.
Cette entité sera votre point de contact avec les autorités cantonales et vous aidera dans vos démarches (dépôt de plainte et première analyse),
et impliquera les experts du Centre opérationnel de sécurité vaudois (SOC) en cas de nécessité.


explique les premières actions à entreprendre en cas d'attaque par rançongiciel.

(logs) de vos équipements, sera une des premières étapes techniques effectuées afin de comprendre l'attaque et son ampleur.

6. **Annoncer l'incident auprès de la Confédération** (NCSC / GovCERT) via le site https://www.report.ncsc.admin.ch/fr/

PS-SEC/202110.01

Direction générale du numérique et des systèmes d'information (DGNSI)

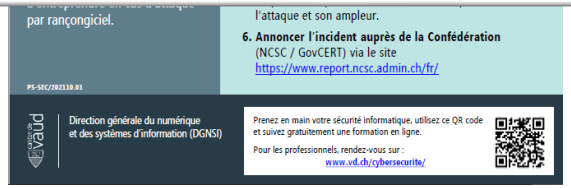
Prenez en main votre sécurité informatique, utilisez ce QR code et suivez gratuitement une formation en ligne.

Pour les professionnels, rendez-vous sur : www.vd.ch/cybersecurite/

Des conseils pour <u>aussi</u> aider les communes ….

3. **Contacter la Police cantonale (117)** et demander

4. **Une cellule de crise** doit être mise en place le plus rapidement possible avec, au minimum, des représentants de l'autorité communale, un responsable de la communication, un responsable informatique et une personne avec des compétences en cybersécurité.



Des conseils pour <u>aussi</u> aider les communes ….

3. Contacter la Police cantonale (117) et demander

4. Une cellule de crise doit être mise en place

5. S'appuyer sur un prestataire spécialisé
en *Incident Response*, qui pourra vous aider dans la gestion technique de l'incident en cybersécurité. La collecte de preuves, via les journaux de connexions (logs) de vos équipements, sera une des premières étapes techniques effectuées afin de comprendre l'attaque et son ampleur.

UNE APPLICATION MOBILE POUR FAIRE FACE AUX CYBER-RISQUES

→ www.vd.ch/cybersecurite

A votre service et belle soirée !

Marc Barbezat – Directeur de la sécurité numérique
Département des infrastructures et des ressources humaines (DIRH)
Direction générale du numérique et des systèmes d'information (DGNSI)
Direction Produits/Services Sécurité
Avenue de Longemalle 1, CH – 1020 Renens
Tél. 021 316 87 00 – Tél. mobile 079 722 37 06
marc.barbezat@vd.ch / www.vd.ch/dgnsi