Bureau d'information et de communication

Rue de la Barre 2
1014 Lausanne

COMMUNIQUÉ DE PRESSE

Exercice de gestion de cybercrise

Renforcer la résilience des infrastructures critiques face aux cybermenaces

Jeudi 5 décembre, un exercice unique de gestion de cybercrise organisé par l'Etat-major cantonal de conduite (EMCC) et la Direction générale du numérique et des systèmes d'information (DGNSI) a impliqué simultanément une centaine d'entités vaudoises en charge d'infrastructures critiques du canton. Essentiel pour renforcer la résilience de telles infrastructures face aux cybermenaces, cet exercice a permis de tester et d'améliorer le fonctionnement et les procédures de réponse des cellules de crise des partenaires impliqués, notamment des communes et le CHUV.

Les nouvelles technologies exposent le Canton à des risques accrus de cyberattaques. Les systèmes critiques, tels que les infrastructures énergétiques et les services publics, sont aujourd'hui les cibles potentielles d'acteurs malveillants sur Internet, avec des motivations très diverses. Les impacts sur l'économie, la santé, l'environnement, la sécurité et le patrimoine qui en découlent peuvent potentiellement être très importants.

Afin de renforcer le niveau de préparation des partenaires clés face à des menaces de plus en plus sophistiquées, le Conseil d'Etat a organisé un exercice de gestion de cybercrise (CYBER 24). Objectifs : évaluer la capacité de réponse en cas de cyberattaque des entités exploitant des infrastructures critiques, renforcer la coordination et la communication entre les différents acteurs impliqués et identifier les points forts et les axes d'amélioration dans la gestion des cybercrises.

Cet exercice a immergé les 95 organisations participantes - notamment le CHUV, l'Alarm receiving center (ARC), la DGNSI, ainsi que plusieurs communes et associations intercommunales - dans un scénario réaliste de cyberattaque, les confrontant à des défis concrets de gestion de crise. Il a offert l'opportunité de mettre en pratique et d'évaluer leurs procédures, tout en générant des documents de référence précieux pour de futures crises. Cette simulation a également permis de tester la coordination et la communication dans les cellules de crise, tout en mettant en lumière leurs points

forts et les domaines nécessitant des améliorations. Après le succès de cette première phase, une extension est prévue en 2025 pour intégrer un scénario de cybercrise majeure au niveau du Canton, sous la direction de l'État-major cantonal de conduite.

Un exercice également au profit de la force cantonale d'intervention cybersécurité

Au-delà de possibilité offerte aux partenaires impliqués d'améliorer leurs propres procédures d'urgence, cet exercice constitue également une base essentielle pour une coopération opérationnelle plus efficace en cas de crise majeure et l'engagement de la force cantonale d'intervention cybersécurité (CSIRT). Pour rappel, cette dernière est opérationnelle depuis le 1er janvier dernier et est composée d'experts en cybersécurité du centre opérationnel de sécurité (SOC) de la Direction générale du numérique et des systèmes d'information (DGNSI). Selon les situations de crise et leur gravité, elle peut être renforcée par les experts de la cybercriminalité de la Police cantonale vaudoise ainsi que par des spécialistes de la gestion de crise de l'EMCC. En cas de situation extraordinaire, la force d'intervention CSIRT déploie une structure de conduite de crise permettant de coordonner les actions et forces en présence pour réduire au maximum les impacts et rétablir la situation au plus vite. Elle apporte aussi son analyse et des points de situation afin que les autorités communales ou la direction de l'entité victime puissent prendre rapidement les meilleures décisions.

En cas de cyberattaque : appeler le 117

En cas de cyberattaque, pour les partenaires en charge d'infrastructures critiques, la procédure est claire : il faut appeler le 117. Les experts de la Police cantonale se mettront ensuite en contact avec la force cantonale d'intervention de la DGNSI, qui coordonnera la suite des opérations.

Bureau d'information et de communication de l'État de Vaud

Lausanne, le 05 décembre 2024

RENSEIGNEMENTS POUR LA PRESSE UNIQUEMENT

DJES, Denis Froidevaux, chef de l'Etat-major cantonal de conduite
DCIRH, Marc Barbezat, Délégué cantonal à la cybersécurité, Direction générale du numérique et des systèmes d'information