|  |  |  |
| --- | --- | --- |
| logo | Règles de filtrage | 1083 |

Responsable :

Mis à jour :

L'accès aux sites Web externes est géré de manière à réduire l'exposition à des contenus malveillants afin de protéger les systèmes d'attaques par des logiciels malveillants et pour empêcher l'accès à des ressources Web non autorisées.

L'organisation s’efforce de réduire les risques liés à l’accès aux sites Web contenant des informations illégales ou connus pour contenir des virus ou du matériel de « *phishing »*.

Une technique pour y parvenir fonctionne en bloquant l'adresse IP ou le domaine du ou des sites Web concernés. Certains navigateurs et technologies anti-malware le font automatiquement ou peuvent être configurés pour le faire.

L’accès est bloqué aux types de sites Web suivants :

* sites Web qui ont une fonction de téléchargement d'informations, sauf autorisation pour des raisons commerciales valables
* sites Web malveillants connus ou suspectés
* serveurs de commande et de contrôle
* site Web malveillant acquis à partir de renseignements sur les menaces
* sites Web partageant des contenus illégaux

Les règles sont établies et tenues à jour pour une utilisation sûre et appropriée des ressources en ligne, y compris toute restriction aux sites Web et applications Web indésirables ou inappropriés.

Une formation est dispensée au personnel sur l'utilisation sécurisée et appropriée des ressources en ligne, y compris l'accès au Web.

La formation inclut les règles de l'organisation, le contact pour signaler les problèmes de sécurité et le processus d'exception lorsque des ressources Web restreintes sont accessibles pour des raisons commerciales légitimes.

Une formation est dispensée au personnel pour s'assurer qu'il n'outrepasse pas un avis de navigateur qui signale qu'un site Web n'est pas sécurisé mais permet à l'utilisateur de continuer.

Le filtrage Web peut inclure la gamme de techniques suivantes :

* des signatures
* une liste de sites Web ou de domaines acceptables
* une liste de sites Web ou de domaines interdits
* une configuration sur mesure pour aider à empêcher les logiciels malveillants et autres activités malveillantes d'attaquer le réseau et les systèmes de l'organisation