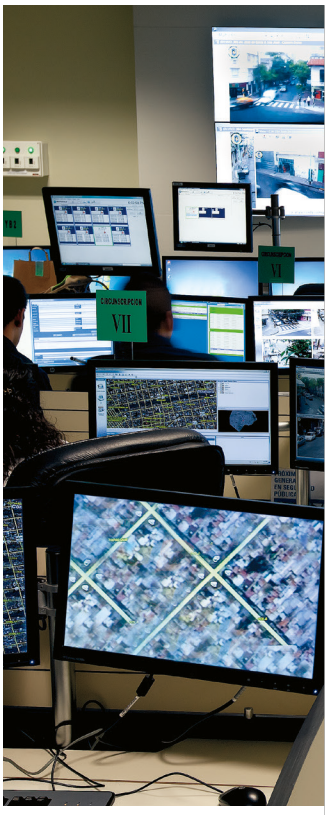
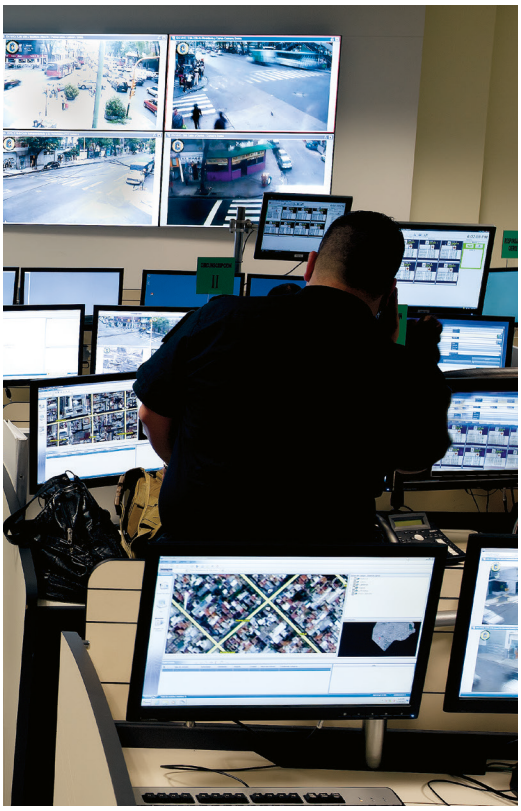


CYBER-RÉSILIENCE : LA NOUVELLE MISSION CRITIQUE POUR LA SÉCURITÉ PUBLIQUE

MOTOROLA SOLUTIONS



La fréquence et la sophistication des cyber-attaques ont augmenté de manière exponentielle, et les entreprises et organisations gouvernementales du monde entier reconnaissent désormais que nul n'est à l'abri. La recherche et la mise en œuvre des meilleures pratiques en matière de cyber-sécurité est devenue une priorité majeure. Les agences de sécurité publique constituent la principale cible pour les cyber-criminels qui cherchent à s'introduire sur leurs réseaux critiques. Les responsables de la sécurité des réseaux informatiques et de communication sont conscients qu'une attaque peut avoir des conséquences graves et des répercutions sur notre vie quotidienne. Toutefois, les moyens de parvenir à la cyber-résilience restent controversés.

Les cyber-menaces et cyber-attaques sont aussi vieilles que l'ordinateur lui-même. En 1986 l'une des premières cyber-intrusions s'est présentée sous la forme d'un simple virus appelé « Brain ». Les effets de cette menace ont été sans conséquences, comparés à celles des attaques malveillantes que l'on connaît aujourd'hui. Avec l'interconnexion des périphériques, des réseaux et des systèmes, les entreprises sont devenues des cibles plus intéressantes. Le secteur des infrastructures critiques, dont les agences de sécurité publique font partie, est désormais la cible privilégiée des cyber-criminels.

Les gouvernements reconnaissent qu'il est essentiel de protéger et de veiller à la pérennité des infrastructures critiques pour assurer leur sécurité, la sécurité publique, la santé et le dynamisme de l'économie. Ils redoublent d'efforts pour mettre en place des infrastructures et des stratégies afin atteindre le niveau de cyber-résilience souhaité.

HAUSSE EXPONENTIELLE DE LA CYBER-ACTIVITÉ DANS LA SÉCURITÉ PUBLIQUE

Au fil des ans, la sécurité publique est devenue l'un des principaux secteurs ciblés avec le plus grand nombre de violations et de pertes de données enregistrées.[1] Les organisations gouvernementales subissent deux fois plus d'attaques que l'ensemble des autres secteurs d'activité. Les attaques en force sont les plus répandues dans le secteur gouvernemental.[2]

Pour les agences de sécurité publique, se doter d'une cyber-résilience fiable est indispensable pour assurer leurs activités quotidiennes. La confidentialité, l'intégrité et la disponibilité des systèmes de communication des missions critiques ne peuvent être diminuées ou compromises. Une cyber-intrusion représente un préjudice qu'aucune agence ne peut se permettre de subir, car elle a un impact direct sur les responsabilités dont elle a la charge au quotidien. Alors, quelles démarches doit d'abord effectuer une agence de sécurité publique ?

76%
LES RSSI DÉCLARENT QUE LES ATTAQUES LANCÉES CONTRE LES INFRASTRUCTURES DEVIENNENT PLUS SOPHISTIQUÉES[3]

CIBLE NO. 1
LE SECTEUR GOUVERNEMENTAL SUBIT LES ATTAQUES LES PLUS DESTRUCTRICES[3]

2X
PLUS D'ATTAQUES LANCÉES CONTRE LES GOUVERNEMENTS PAR RAPPORT AUX AUTRES SECTEURS D'ACTIVITÉ[2]

QUE PROTÉGEZ-VOUS, ET CONTRE QUI ?

Les pays définissent des structures nécessaires à la mise en œuvre de programmes de cyber-sécurité complets, permettant de réduire les risques et de protéger les infrastructures critiques, les institutions ou les entreprises. De l'initiative « Cybersecurity Framework » du National Institute of Standards and Technology (NIST) aux États-Unis au cadre stratégique de cyber-défense de l'UE en Europe, les éléments essentiels de la cyber-sécurité sont définis et associés à des normes éprouvées que les organisations sont invitées à étudier. Compte tenu du volume énorme de ressources de la sécurité publique qui doit être protégé, la complexité de la tâche peut sembler insurmontable.

Au moment où les agences de sécurité publique et les organismes gouvernementaux se concentrent sur le choix de leurs infrastructures, ils ne peuvent pas se permettre de perdre de vue les principes fondamentaux. Ils doivent tout d'abord se poser deux questions "Que protégeons nous ?" et"De qui nous protégeons nous ?" avant d'élaborer et de mettre en œuvre une stratégie. Il est essentiel de répondre à ces questions pour prendre des mesures efficaces face à un environnement de cyber-sécurité en perpétuelle évolution.

EN FINIR AVEC LE MYTHE DU RÉSEAU FERMÉ

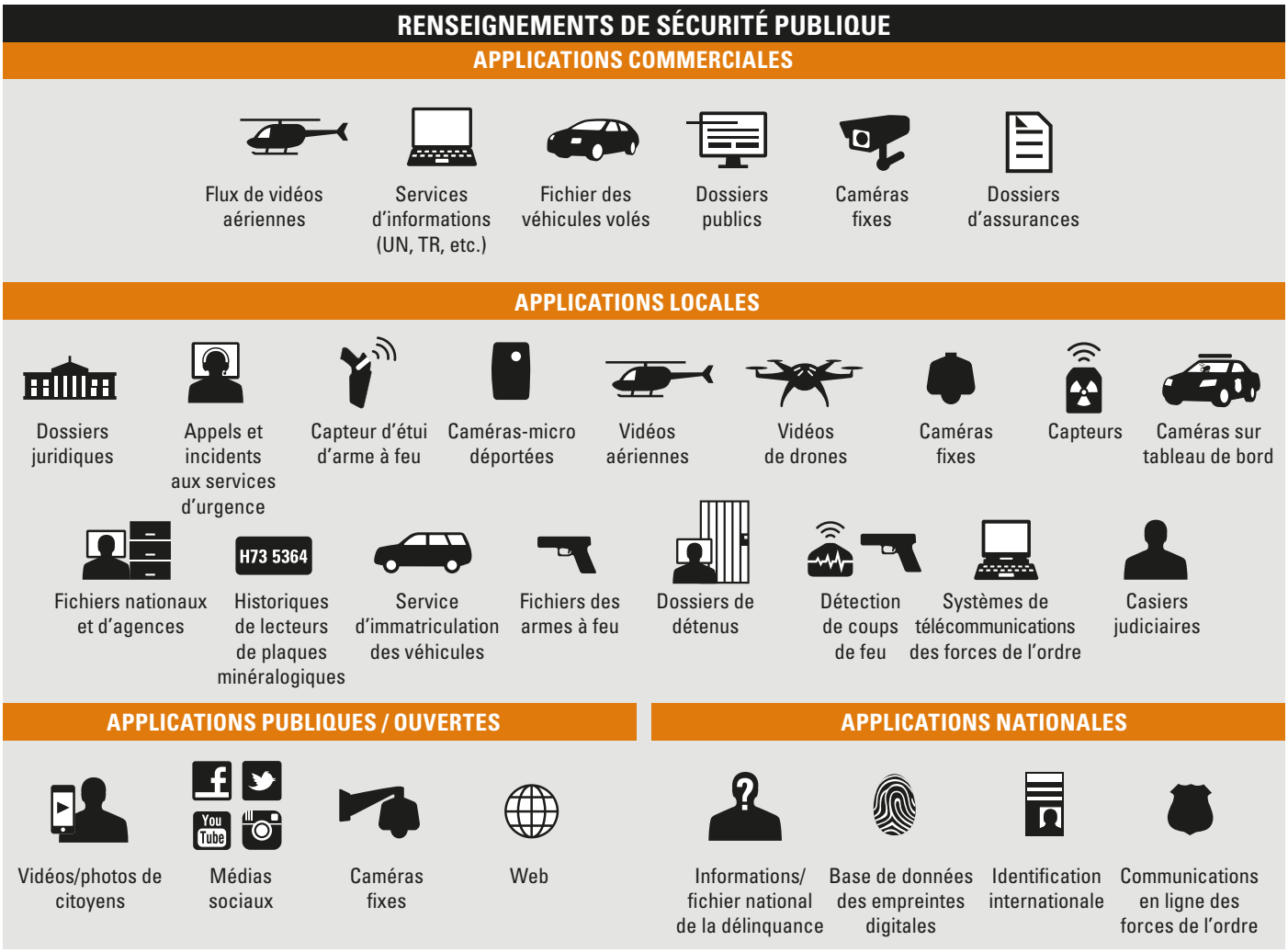
Pendant des décennies, les agences de sécurité publique ont pu apprécier les avantages d'un réseau « fermé » et « sécurisé » au sein de leur environnement opérationnel. Avec l'évolution rapide de la technologie et des nouveaux flux de données (médias sociaux, caméras-micro déportées, police intelligente – voir la Figure 1), le luxe d'un réseau fermé est depuis longtemps révolu. Les réseaux de sécurité publique sont interconnectés et les informations des missions critiques qu'ils contiennent sont très recherchées par les criminels.

La question n'est plus de savoir si une cyber-attaque aura lieu, mais quand et comment elle interviendra et quelles en seront les conséquences.

DES ATTAQUES NOMBREUSES, INTENTIONNELLES OU INVOLONTAIRES

Les pirates attaquent les organismes publics dans le but de perturber les services, d'acquérir des informations critiques et de créer une forme de terrorisme. Ces incidents mobilisent fréquemment les responsables des systèmes d'information jusque tard dans la nuit. Au cours de l'année passée, leurs préoccupations n'ont cessé d'augmenter ; 37 % citent les attaques contre l'État-nation, 24 % la guerre de l'information et/ou le cyber-terrorisme et 15 % les violations impliquant des informations à forte valeur ajoutée.[4] Les personnes responsables de la sécurité des informations critiques doivent prêter attention à l'augmentation sensible des cyber-attaques lancées contre les agences de sécurité publique.

Les agences de sécurité publique doivent également prendre les menaces internes très au sérieux. Les menaces internes – c'est-à-dire celles émanant d'individus disposant d'un accès immédiat aux réseaux « fermés » – sont souvent dues à des actes involontaires, des erreurs humaines et des mauvaises pratiques. Près d'un tiers des personnes interrogées déclarent que les actes criminels commis par le personnel interne sont plus coûteux ou plus dommageables que les incidents dus à des individus extérieurs aux agences de sécurité publique.[5] Les cyber-crimes les plus coûteux sont dus à des actes malveillance internes, aux attaques par déni de services et aux attaques lancées depuis le Web ; ces catégories représentent pas moins de 55 pour cent des coûts imputables à la cyber-criminalité par entreprise et par an.[6]



ÉTUDIER DE PLUS PRÈS LES MENACES INTERNES

Qu'il s'agisse de l'intrusion délibérée d'un ancien technicien sur un réseau ou de l'injection accidentelle d'un logiciel malveillant par un employé en poste, les agences de sécurité publique doivent être proactives et prêtes à répondre au nombre croissant d'attaques internes.

ATTAQUES INTERNES

Un employé mécontent a accès à des informations confidentielles concernant un réseau de communication radio pour les missions critiques. Il transmet par SMS la configuration du système à des personnes malveillantes extérieures, afin de perturber les communications.

ACTIONS

Réexaminez régulièrement les règles de l'organisation (notamment celles liées à la consultation et le traitement des renseignements confidentiels, ainsi qu'à l'utilisation des appareils de communication personnels) avec le service juridique, les relations humaines et les employés.

Envisagez le déploiement de technologies et de pratiques pour contrôler le comportement de manière à mettre en place une surveillance légale des employés ayant accès à des informations confidentielles.

Formez le personnel et mettez en œuvre des processus de contrôle du réseau. Envisagez le déploiement de technologies Honeypot pour piéger les cyber-pirates et surveillez continuellement votre réseau afin de déceler toute anomalie.

PROPAGATION DE LOGICIELS MALVEILLANTS

Sans le savoir, un répartiteur apporte une clé USB infectée – un périphérique autorisé par la politique BYOD (Bring You Own Device) de l'agence – sur son lieu de travail. Un logiciel malveillant se propage sur le réseau, désactive les postes de répartition et contamine d'autres agences.

ACTIONS

Mettez continuellement à jour vos logiciels anti-malware.
Renforcez votre système et installez les correctifs requis.
Réexaminez régulièrement les listes de contrôle d'accès des routeurs et les règles des pare-feux.
Surveillez le système afin de détecter tout programme malveillant ou autre activité inhabituelle.
Réagissez immédiatement pour neutraliser l'infection et limiter sa propagation.

CONNEXION NON AUTORISÉE

Un technicien informatique installe un point d'accès Wi-Fi non autorisé et non sécurisé pour lui facilité l'accès à distance aux systèmes de son agence. Le point d'accès Wi-Fi devient un vecteur d'attaque qui est découvert par des individus malveillants.

ACTIONS

Activez les contrôles de sécurité sur les ports des commutateurs réseau.
Renforcez les systèmes afin d'éviter toute activation non autorisée d'interfaces Wi-Fi sur les serveurs et les périphériques d'utilisateurs finaux.
Surveillez le système afin d'identifier tout ajout non autorisé sur le réseau.
Surveillez le réseau afin d'identifier tout trafic réseau inhabituel.

38%
DES INTRUSIONS SONT DÉTECTÉES SUR LES RÉSEAUX GOUVERNEMENTAUX[7]

55%
DU COÛT DE LA CYBER-CRIMINALITÉ IMPUTABLE À LA MALVEILLANCE D'EMPLOYÉS INTERNES, AUX ATTAQUES PAR DÉNI DE SERVICE ET LANCÉES DEPUIS LE WEB[6]

31 JOURS
C'EST LE DÉLAI MOYEN POUR CONTENIR UNE ATTAQUE[6]

SIMPLIFIER LE RISQUE ET L'EXÉCUTION POUR UN IMPACT MAXIMAL

Les agences de sécurité publique peuvent simplifier leurs structures de gestion du risque en concentrant leurs efforts sur les principales composantes qui permettent de garantir la continuité et l'intégrité opérationnelle de leurs services critiques :

1. Un modèle simplifié de gouvernance et surveillance doit tenir compte des éléments constitutifs de l'écosystème tels que les personnes, les processus, les réglementations et les technologies. Ils ne peuvent pas individuellement protéger l'environnement critique mais peuvent y parvenir en travaillant ensemble de manière cohérente.

2. Le périmètre simplifié de la gestion du risque doit permettre d'identifier clairement les risques techniques concrets et les solutions pour les atténuer. Ces risques doivent être classés de manière factuelle et spécifique.

3. Le modèle d'exécution simplifié doit se concentrer sur les zones à risque définies au sein de toutes les entités organisationnelles, et ne doit pas être surchargé par les actions de mise en conformité nécessitant des ressources importantes. Dans la plupart des cas, les objectifs de conformité seront atteints de manière transparente lorsque les aspects pratiques de la gestion du risque auront été traités.

Par exemple, lorsque les agences de sécurité publique renforcent leurs systèmes conformément aux meilleures pratiques les plus exigeantes préconisées dans le secteur, à l'image des directives DISA STIG ou NIST 800-53, elles peuvent satisfaire à des règles de conformité moins strictes, tout en remédiant aux risques techniques les plus critiques.

SIMPLIFIER LE PÉRIMÈTRE DE LA GESTION DU RISQUE

Commencez par déterminer ce que vous devez vraiment protéger – les données des missions critiques, la solidité de l'intégrité opérationnelle ou d'autres éléments. Évaluez votre compréhension des menaces et des risques potentiels affectant l'activité de votre entreprise– des dépendances vis à vis de tiers aux menaces internes.

Ensuite, demandez-vous contre qui vous protégez votre entreprise. Analysez plus particulièrement les vecteurs d'attaque possibles, la probabilité de subir une attaque et l'ensemble de compétences requises pour lancer une attaque contre votre système.

Après avoir identifié les systèmes et ressources connexes, l'étape suivante consiste à évaluer vos capacités fondamentales en matière de cyber-sécurité et de déploiement. Il est essentiel de simplifier le périmètre et de définir clairement un mode de déploiement permettant d'atteindre vos objectifs de conformité en fonction des risques techniques.

PRIVILÉGIEZ LA SURVEILLANCE ET LA RÉACTIVITÉ, ET NON LA CONSTRUCTION DE FORTERESSES

La plupart des adversaires utilisent une approche très simple pour s'introduire dans les systèmes et sont souvent actifs plusieurs mois sur un réseau compromis avant d'être détectés. En moyenne, les pirates informatiques passent 243 jours sur le réseau d'une victime avant d'être repérés.[8] Néanmoins, les agences concentrent leurs recherches aux mauvais endroits ; ce qui revient concrètement à sécuriser les fenêtres et laisser les portes grandes ouvertes.

Même lorsque les agences de sécurité publique sont en conformité avec à toutes les contraintes réglementaires, une erreur apparemment anodine peut mener à une intrusion, provoquer des effets en cascade et compromettre les opérations des missions critiques. Une entreprise conforme à 100 % peut être compromise le jour même.

Au lieu de construire des forteresses dans le but de protéger le périmètre et les autres ressources, les agences de sécurité publique peuvent prendre des mesures efficaces en réalisant une étude de faisabilité sur un contrôle fiable et exhaustif de leurs capacités en matière de sécurité et de réaction en cas d'incident.

ADOPTEZ UNE APPROCHE HOLISTIQUE POUR SÉCURISER VOTRE INFRASTRUCTURE CRITIQUE

ANALYSE ET ÉVALUATION : identifiez et classifiez les ressources, puis évaluez et hiérarchisez les vulnérabilités

IMPACT: construisez une infrastructure bien définie pour établir des priorités et des procédures et l'affectation des fonds pour limiter des risques

ACTION CORRECTIVE : mettez en place un plan systématique pour remédier aux risques, garantir la continuité des services et gérer la reprise en cas de sinistre

VIGILANCE : procédez à l'évaluation continue des risques et à l'élaboration de processus rentables

CONSEILLER DE CONFIANCE : collaborez avec des experts du secteur pour créer un écosystème sécuritaire dans lequel toutes les entités collaborent pour garantir une protection totale

LA SÉCURITÉ C'EST CE QUE VOUS NE VOYEZ PAS. LE SAVOIR-FAIRE C'EST CE QUE VOUS NE POUVEZ PAS IGNORER.

Motorola est le leader mondial des communications pour les missions critiques dans plus de 100 pays, nous avons donc parfaitement conscience qu'il est essentiel de concevoir, développer et déployer des technologies totalement efficaces et sécurisées. Nous collaborons avec des agences de sécurité publique à travers le monde pour relever les défis liés à la cyber sécurité. Nous travaillons en partenariat avec leurs ressources internes, afin de leur fournir la formation et les outils pour les aider à devenir cyber résilient dans un climat de menace croissante.

SOURCES

1. 2015 Data Breach Investigation Report, Verizon Wireless
2. 7. Post-Intrusion Report, Vectra, June 2015
3. Report on Cybersecurity and Critical Infrastructure in the Americas, Trend Micro, 2015
4. 6. 2015 Ponemon Global Megatrends Report
5. Managing cyber risks in an interconnected world, PWC, September 2014
8. Cybersecurity Roadshow, IBM 2014

Pour découvrir comment Motorola aide les agences de sécurité publique à travailler plus efficacement, plus intelligemment et plus rapidement grâce aux technologies de nouvelle génération, consultez le site Web **motorolasolutions.com/cybersecurity**

Motorola Solutions France SAS, Parc Les Algorithmes, Saint Aubin, 91193 France, Tel: +33 1 69 35 77 00 **motorolasolutions.fr**

MOTOROLA