

# Infrastructures critiques



# Introduction

Une des grandes forces des sociétés évoluées actuelles est aussi l'une de leurs grandes faiblesses. Dans notre environnement hyperconnecté, les sociétés développées et hautement technologiques sont largement dépendantes d'un ensemble de services désormais essentiels.

Certaines infrastructures constituent la base du fonctionnement normal des systèmes de production et des services fondamentaux de n'importe quelle société. Une quelconque interruption, qu'elle soit imputable à des causes naturelles, une défaillance technique ou une attaque délibérée, aurait alors des conséquences graves pour les approvisionnements vitaux ou le fonctionnement de services essentiels, sans parler de la menace pour la sécurité.

Ces dernières années, la cybercriminalité n'a cessé de s'étendre autour du globe. Le développement de la connectivité et la mutation numérique de la société représentent une épée à double tranchant, car ils offrent un moyen d'action pour les criminels. Mais que se passe-t-il lorsque les réseaux que nous considérons comme essentiels à notre existence deviennent la cible d'une activité criminelle ?





# Secteurs sensibles et infrastructures critiques

La protection des infrastructures critiques est une préoccupation pour tous les pays. Le haut niveau de développement des sociétés modernes est largement tributaire d'un ensemble de services de base et essentiels fournis, dans une large mesure, par le secteur privé.

Jamais les infrastructures n'ont été aussi cruciales pour le fonctionnement normal des services et systèmes qui soutiennent la production, notamment les systèmes des administrations, d'alimentation en eau, les systèmes financiers et fiscaux, ou encore ceux utilisés dans les domaines de l'énergie, de l'aérospatiale, du nucléaire et des transports.

**Les infrastructures que nous considérons comme critiques incluent les installations, réseaux, services et systèmes qui, s'ils devaient être interrompus d'une manière ou d'une autre, affecteraient la santé, la sécurité et le bien-être général des citoyens d'un pays.**

Garantir la fourniture de ces services de base face aux nouvelles menaces n'est pas seulement la responsabilité des administrations

# Caractéristiques techniques

Du fait de certaines caractéristiques techniques et du niveau d'exposition des données sur ces réseaux, leur protection n'est pas une tâche ordinaire.



**Les nouvelles intrusions ciblant les systèmes cyber-physiques des processus industriels qui s'exécutent sur les infrastructures critiques ont rendu nécessaire l'adoption de nouvelles stratégies afin de détecter ces menaces sans interférer avec le fonctionnement de l'infrastructure.**



## Architecture hybride

D'une part, de nombreuses infrastructures définies comme critiques reposent sur une architecture hybride associant les réseaux informatiques (IT) classiques et les réseaux de technologies opérationnelles (OT) qui administrent les composants interagissant avec les supports physiques (systèmes cyber-physiques).



## Systèmes isolés de l'Internet

Ce point mérite une certaine attention, car la tendance croissante à l'interconnexion de tous les types d'infrastructures multiplie aussi les vecteurs d'attaque possibles. Les systèmes de contrôle-commande de telles infrastructures sont normalement isolés d'Internet et communiquent sur un réseau interne.



## SCADA

Néanmoins, certains systèmes de contrôle-commande SCADA sont visibles sur Internet, voire même accessibles par ce biais. La majorité de ces systèmes n'ont pas de relation directe avec les systèmes de gestion des infrastructures critiques, mais ils pourraient servir de passerelle permettant à un pirate de dérober des informations confidentielles à même de faciliter une attaque plus sophistiquée.

# Les types d'attaques visant les infrastructures critiques

Les nations modernes sont confrontées à de nombreux défis en matière de sécurité nationale. Les priorités stratégiques dans ce domaine incluent les infrastructures exposées à une série de menaces. Pour sécuriser ces infrastructures, il est essentiel d'élaborer un plan qui inclut la prévention et la protection contre les menaces potentielles, tant en matière de sécurité physique que de technologie et de communications.

Ces dernières années, une série d'événements cruciaux, tels que les attentats du 11 septembre, ont marqué un tournant pour la sécurité mondiale. Cette période a vu l'émergence d'un nouveau paysage dans lequel la destruction de certaines cibles pourrait porter atteinte à la vie, à la santé et au bien-être d'individus et de nations entières.

La manière traditionnelle d'envisager la sécurité de telles cibles a évolué. Jusqu'alors, la sécurité relevait du domaine public et de la seule responsabilité des administrations. Désormais, les infrastructures critiques sont largement entre

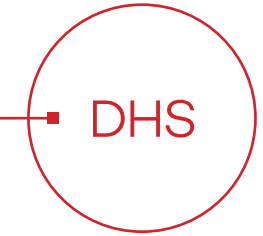
les mains du secteur privé et celui-ci a donc une responsabilité dans ce domaine. Après le 11 septembre, les États-Unis ont réagi en créant le Department of Homeland Security (Département de la Sécurité intérieure) et en instaurant un ensemble de réglementations d'une portée étendue.

En Europe, une initiative similaire a vu le jour après le 11 mars 2004, date des attentats à la bombe dans plusieurs trains à Madrid. La Commission européenne a élaboré une stratégie globale pour la protection des infrastructures critiques, intitulée 'Programme européen de protection des infrastructures critiques'. Ce programme inclut des propositions visant à améliorer, en Europe, la prévention, la préparation et la réponse face à des attaques terroristes.

Entre autres aspects, la directive stipule que la responsabilité principale et finale de la protection des infrastructures critiques incombe aux états membres et aux opérateurs des dites infrastructures, et elle exhorte chaque nation à mettre en œuvre une série d'actions et d'initiatives dans sa législation nationale.

---

11S  
EEUU



DHS

11M  
Europe



PEPIC

# Historique de certaines attaques

Le grand public est convaincu de l'existence de risques mais il croit, qu'en réalité, les cyber-attaques contre les infrastructures critiques sont peu nombreuses. Malheureusement, la réalité est tout autre et les cas documentés dans le monde se comptent par centaines. Les attaques contre ces réseaux existent depuis des décennies et vous trouverez ci-après un résumé de certaines d'entre elles.

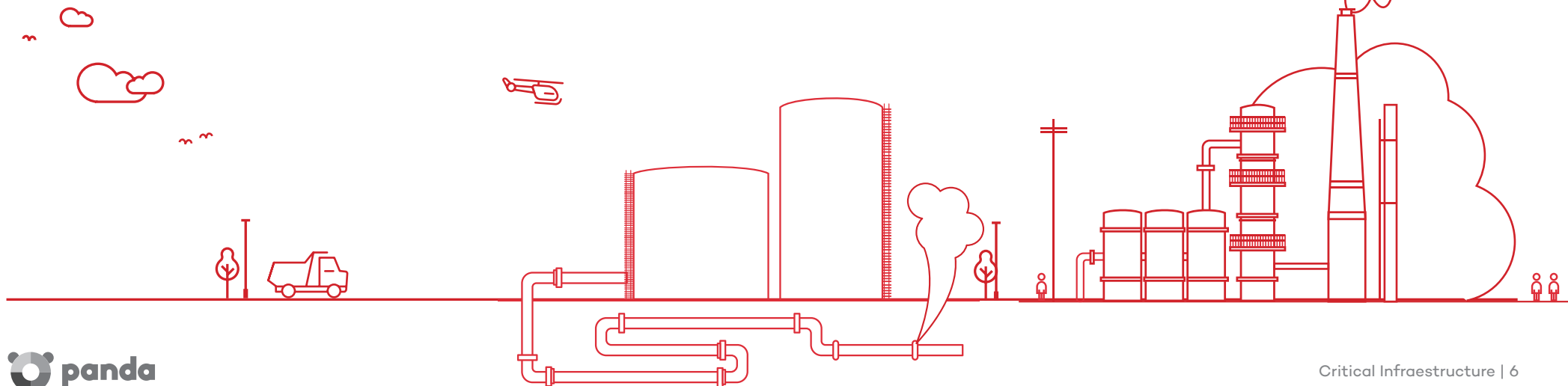
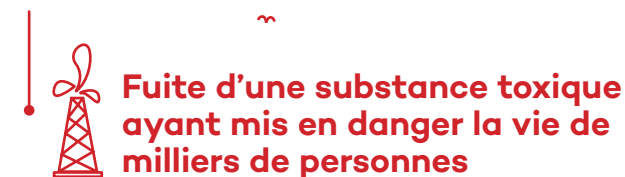
## Oléoduc sibérien

Le terme Internet vient immédiatement à l'esprit lorsqu'il est question de cyber-attaques contre des infrastructures critiques. Pourtant, la toute première cyber-attaque a eu lieu en **1982**, bien avant la naissance d'Internet. Un groupe de pirates avait réussi à installer un cheval de Troie sur un système SCADA qui contrôlait l'oléoduc sibérien, provoquant alors une gigantesque explosion. L'attaque avait été orchestrée par la CIA, bien que cette information n'ait été révélée qu'en 2004, lorsque Thomas C. Reed, ex-secrétaire du Département de la Défense des États-Unis et conseiller de Ronald Reagan a publié le livre « At the Abyss: An Insider's History of the Cold War ».



## Chevron

L'incident suivant s'est déroulé près de dix ans plus tard, en **1992**, lorsqu'un employé de la compagnie pétrolière Chevron a été licencié après avoir piraté les ordinateurs responsables des systèmes d'alerte sur les sites de New York et de San Jose. Cet employé les avait reconfigurés pour qu'ils tombent en panne au démarrage du système. Il a fallu attendre la fuite d'une substance toxique à Richmond, en Californie, pour découvrir le sabotage. Le système n'a pas généré l'alerte correspondante, ce qui a mis en danger la vie de milliers de personnes pendant les dix heures qu'a duré la panne du système.



## Projet Salt River


En août **1994**, Lane Jarret Davies a réussi à pirater le réseau du Salt River Project via un modem. Il a accédé à des informations et a supprimé des fichiers du système chargé de la surveillance et de l'approvisionnement en eau et en électricité. Il a aussi réussi à accéder à des informations personnelles et financières des clients et employés de la société.

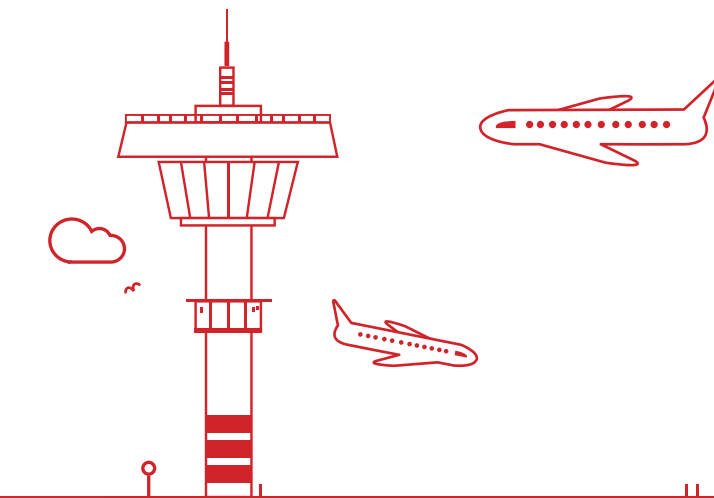
 **Suppression de fichiers dans le système responsable de la surveillance et de l'approvisionnement en eau et en électricité**



## Worcester Airport

D'autres secteurs clés ont aussi souffert d'attaques ciblées. Le 10 mars **1997**, un pirate s'est introduit dans le système utilisé pour les communications de contrôle du trafic aérien à Worcester, dans le Massachusetts. Il a provoqué une défaillance qui a mis le système téléphonique hors service pendant six heures. Il a plus précisément affecté le système téléphonique de la tour de contrôle, le service d'incendie de l'aéroport et les compagnies aériennes présentes dans les locaux de l'aéroport.

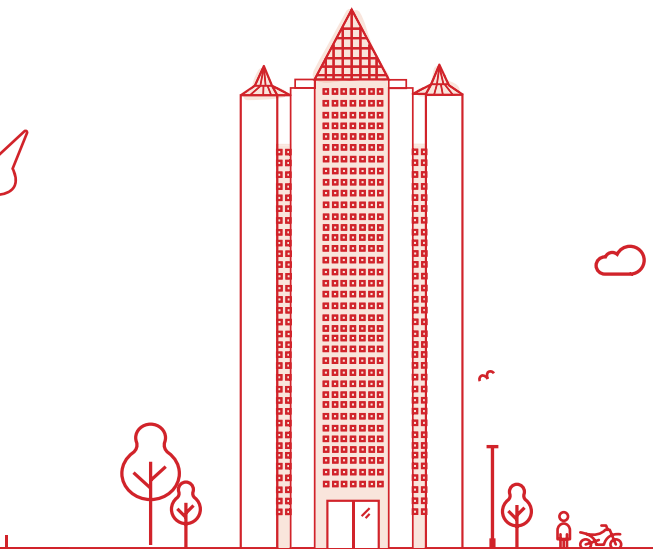
 **Défaillance affectant pendant 6 heures le système téléphonique de la tour de contrôle, le service d'incendie de l'aéroport et les compagnies aériennes présentes dans les locaux de l'aéroport de Worcester.**



## Gazprom

En **1999**, un pirate a mis en échec les systèmes de sécurité de Gazprom, le géant russe de l'énergie. Grâce à des complicités en interne, il a utilisé un cheval de Troie pour prendre le contrôle du système SCADA pilotant l'acheminement du gaz. Heureusement, il n'y a pas eu de conséquences graves et le service a été restauré rapidement.

 **Des pirates prennent le contrôle du système Gazprom pilotant l'acheminement du gaz.**



## Station de distribution d'eau Maroochy

Un ex-employé de Maroochy Water System a été condamné à une peine de prison de deux ans après avoir utilisé du matériel volé en 2000 pour pirater le système de contrôle de l'eau avec pour conséquence de répandre un million de litres d'eaux usées dans une rivière avoisinante, inondant à cette occasion un hôtel.



**Déversement d'un million de litres d'eaux usées dans une rivière.**

## Usine de traitement de gaz

Une usine de traitement de gaz exploitée par une compagnie pétrolière américaine a également subi une attaque en 2001. L'enquête, qui a duré six mois, a révélé que l'attaque était le fait d'un fournisseur qui, afin de couvrir une erreur qu'il avait provoqué sur un ordinateur, avait fait diversion en piratant trois ordinateurs de la compagnie et en provoquant une interruption de l'approvisionnement de foyers et d'entreprises dans un pays européen.



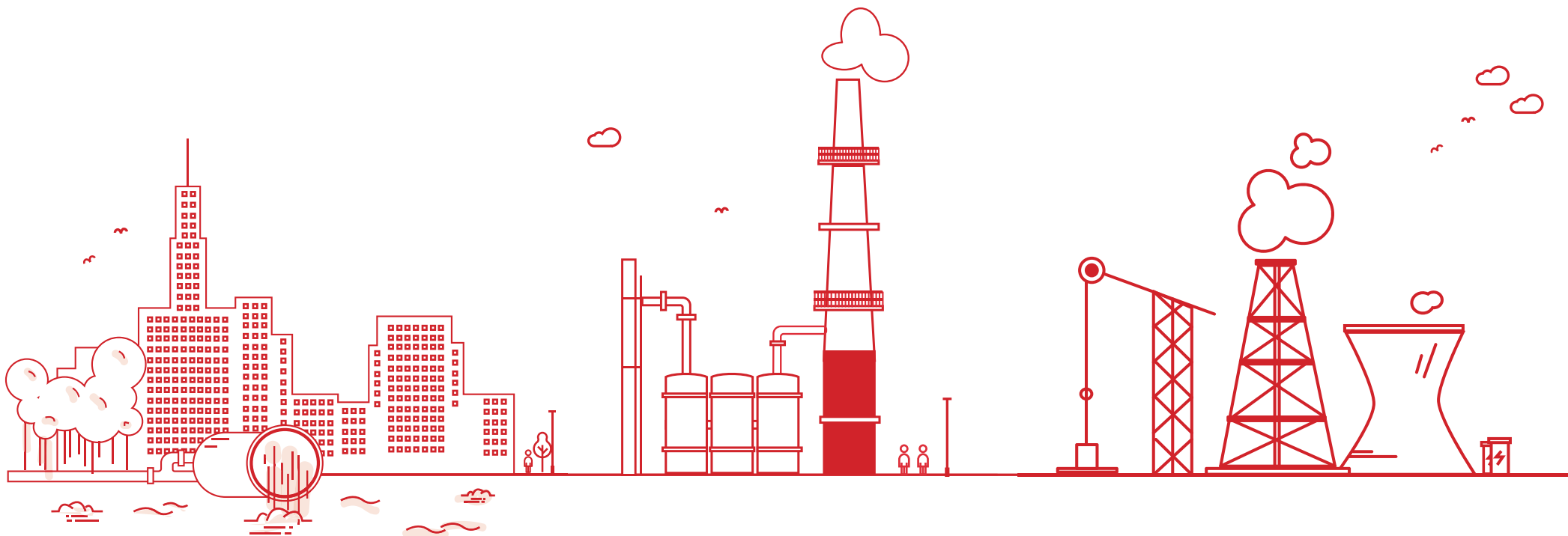
**Une cyber-attaque interrompt l'approvisionnement en gaz de foyers et d'entreprises dans un pays européen.**

## PDVSA

En décembre 2002, la compagnie pétrolière vénézuélienne PDVSA a été la cible d'une attaque qui a réduit la production de 3 millions à 370 000 barils par jour. L'attaque menée contre plusieurs ordinateurs de la compagnie a eu lieu alors que le personnel était en grève, laissant à penser qu'elle avait pu être l'œuvre d'employés.



**Une attaque réduit la production de pétrole de 3 millions de barils par jour à 370 000.**





## Feux de circulation de la ville de Los Angeles

En **2006**, deux ingénieurs de la circulation de Los Angeles ont piraté les feux de circulation de la ville pendant une manifestation. Ils ont réussi à modifier la programmation de certains feux à des carrefours stratégiques, afin qu'ils restent au rouge et provoquent des embouteillages monstres.



**Un piratage provoque des embouteillages monstres**

## Réseau de tramway de la ville de Lodz.

En **2008**, un étudiant de 14 ans a piraté les systèmes du réseau de tramway de la ville de Lodz en Pologne. Le bilan : déraillement de quatre voitures et 12 blessés. L'étudiant avait fabriqué une télécommande à infrarouge, similaire à une télécommande TV, et il s'en était servi pour commander les aiguillages.



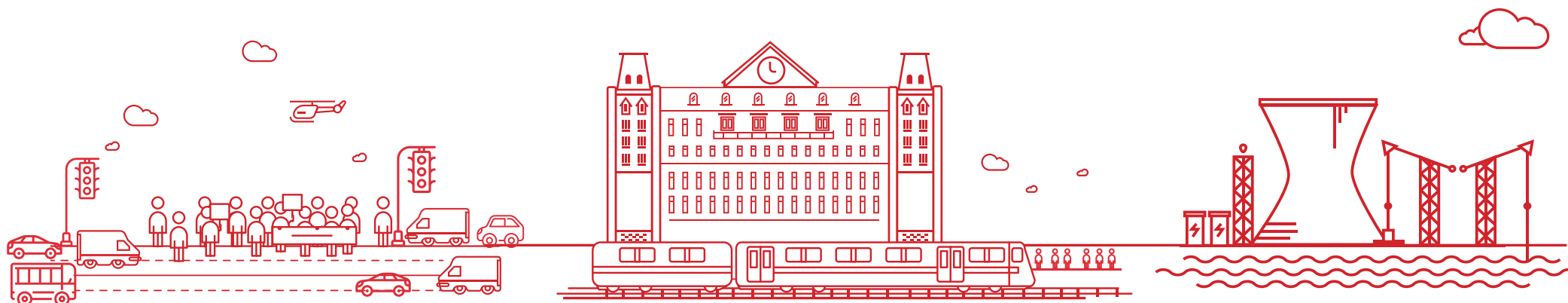
**Une cyber-attaque fait dérailler quatre voitures d'un tramway et blesse 12 personnes**

## Saudi Aramco

En **2012**, la plus grande compagnie pétrolière au monde, Saudi Aramco, a été victime d'une attaque ciblée contre son siège social. Les pirates sont parvenus à pénétrer sur le réseau via une attaque contre un de ses employés et, de là, ont accédé à 30 000 ordinateurs de la compagnie. À un certain stade, les pirates ont même réussi à supprimer le contenu de tous les ordinateurs piratés tandis que l'écran affichait un drapeau américain en flammes. Un groupe, se faisant appeler « Cutting Sword of Justice » (L'Épée tranchante de la justice), a revendiqué l'attaque.



**Suppression du contenu de tous les ordinateurs d'une entreprise et affichage d'un drapeau américain en flammes sur les écrans**



## Ram Gas

Deux semaines seulement après l'attaque contre Saudi Aramco, la compagnie qatari RamGas, qui est le deuxième plus grand producteur mondial de gaz naturel liquéfié, a été attaquée au moyen du même logiciel malveillant employé contre la compagnie pétrolière saoudienne. Plusieurs jours durant, le réseau interne de la compagnie et son site Web ont été hors service.



**Une attaque met hors service le réseau interne d'une compagnie et son site Web**

## Usine métallurgique en Allemagne.

En **2014**, une usine métallurgique en Allemagne a aussi été victime d'une attaque. Par le biais de techniques d'ingénierie sociale, les pirates ont réussi à accéder via l'ordinateur d'un employé, au réseau interne du système de contrôle-commande. Suite à cela, il est devenu impossible d'arrêter un des hauts fourneaux, ce qui a provoqué des dégâts importants à l'usine.



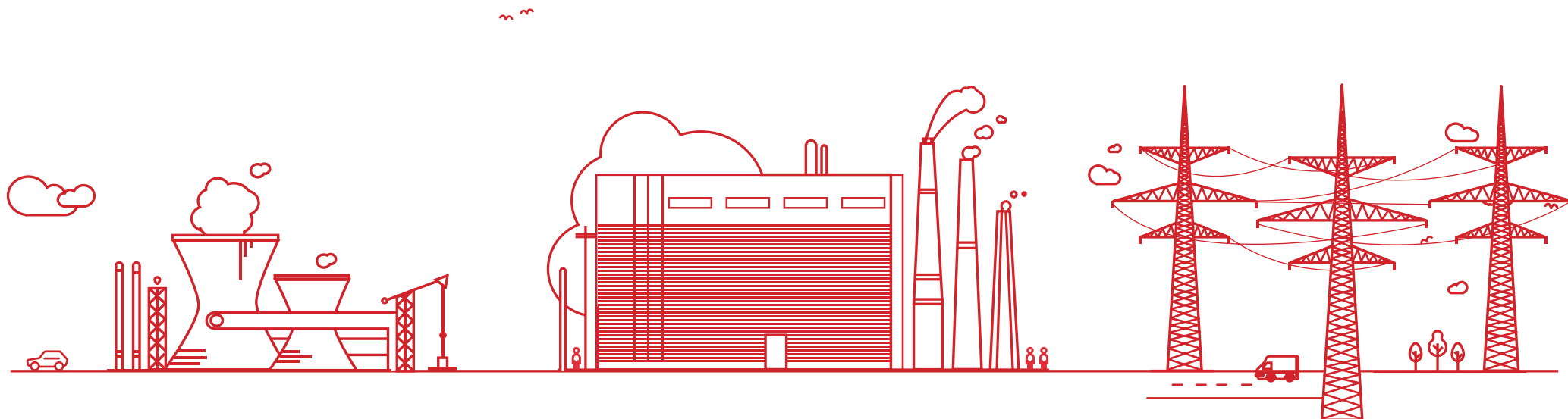
**Une cyber-attaque provoque des dégâts importants dans une usine métallurgique**

## Réseau d'électricité de l'Ukraine.

Fin **2015**, l'Ukraine a été victime d'une cyber-attaque contre son réseau national d'électricité et plus de 600 000 foyers ont été privés de courant.



**Une cyber-attaque prive d'électricité 600 000 foyers ukrainiens**



## La première cyber-attaque de l'histoire contre l'infrastructure Internet.

Malgré cette longue liste d'incidents, la première cyber-attaque de l'histoire contre l'infrastructure Internet dans un pays a eu lieu le 27 avril **2007**, quand une série d'attaques en Estonie a mis hors service de nombreux sites Web appartenant à



une multitude d'organisations. Notamment le parlement, des ministères, des banques, des journaux et d'autres médias, etc.

L'attaque a également ciblé certaines adresses peu médiatisées, dont le système de traitement des ordres financiers du pays et ses services de télécommunications. Urmas Paet, le ministre des Affaires Etrangères estonien, a accusé publiquement le gouvernement russe d'être derrière les attaques, même s'il n'a pu produire de preuves pour soutenir cette allégation.

## Les cas les plus notoires de cyber-attaques contre des infrastructures critiques : Stuxnet

En **2008**, nous avons été témoins d'une des cyber-attaques les plus célèbres de l'histoire contre des infrastructures critiques : **Stuxnet**. Il est maintenant avéré qu'il s'agissait d'une



attaque coordonnée des services secrets israéliens et américains visant à saboter le programme nucléaire iranien.

Les agresseurs ont créé un ver visant à infecter les ordinateurs contrôlant les centrifugeuses d'enrichissement d'uranium de la centrale iranienne de Natanz. Le ver a provoqué l'emballement et la destruction de toutes les centrifugeuse de la centrale, tout en manipulant les affichages de données afin que les ingénieurs ne se doutent de rien. Ce cas, très médiatisé, a contribué à la prise de conscience de ce type de menaces par le grand public.



## Les attaques courantes dans les autres entreprises se produisent aussi dans ces installations

Outre les attaques visant spécifiquement à saboter ce type d'infrastructure, les attaques similaires à celles dont souffrent d'autres entreprises affectent aussi ces installations et les conséquences ont, parfois, été aussi graves que celles des attaques ciblées. **Ces types de problèmes ont, pour l'essentiel, fait leur apparition au début de la dernière décennie, lorsque les vers réseau ont commencé à se propager.**

L'infection virale suivante, qui a coûté des milliers de dollars à une grande usine américaine de productions d'aliments, en constitue un exemple. Un des employés de l'usine s'est connecté à distance à partir de son domicile. Son ordinateur était infecté par le virus Nimda. Par conséquent, dès qu'il a accédé au réseau de l'entreprise, le ver s'est propagé à tous les systèmes de contrôle-commande.

En 2003, une compagnie pétrolière américaine a subi les conséquences du ver SQLSlammer lorsque celui-ci a pénétré sur l'intranet de l'entreprise. Même s'il n'a pas provoqué l'arrêt de la production, il a affecté les communications internes. Il a fallu plusieurs jours pour l'éliminer complètement du réseau et pour mettre à jour les systèmes afin de prévenir d'autres attaques.

Ce ver a, en fait, été l'un des plus perturbateurs pour les entreprises.

Pour se propager, il a exploité une vulnérabilité des serveurs de base de données SQL (un outil très répandu dans les environnements d'entreprises). La vulnérabilité a été corrigée par Microsoft en janvier 2003 et, dans ce cadre, une autre compagnie pétrolière américaine a commencé à mettre à jour toutes ses installations dès la sortie du correctif, afin de se prémunir contre le ver. Toutefois, pour terminer l'installation, il fallait redémarrer les serveurs sur lesquels le correctif avait été appliqué. Mais, comme plusieurs serveurs étaient situés sur des plates-formes pétrolières sans personnel informatique dédié, cette opération a dû être supervisée par des personnels spécialisés dépêchés par hélicoptère. Pendant le processus, le ver s'est infiltré sur certains systèmes de l'entreprise et ceux qui n'avaient pas été redémarrés ont été infectés.

En 2003, un des plus grands constructeurs automobiles américains a également subi une attaque du ver SQLSlammer, laquelle s'est propagée rapidement et a touché 17 de ses sites de production. Coût total pour le constructeur : 150 millions de dollars US. Alors que le correctif était disponible depuis six mois, les responsables informatiques de l'entreprise ne l'avaient pas appliqué.

La même année, une infection par un code malveillant (le logiciel responsable de l'incident n'a pas été rendu public) a affecté un ordinateur d'Air Canada assurant la gestion des informations de vol, des ravitaillements en carburant, etc. Suite à

l'infection, 200 vols ont été retardés ou annulés.

En 2005, au Japon, l'ordinateur d'un employé de Mitsubishi Electric a été infecté par un logiciel malveillant, ce qui a abouti à la fuite de documents d'inspection confidentiels de deux centrales nucléaires conçues par l'entreprise.

En 2006, deux ordinateurs d'un hôpital britannique chargés de la gestion du traitement par radiothérapie de patients atteints du cancer ont été infectés par un logiciel malveillant. Le traitement de 80 patients a dû être retardé. Quelques années plus tard, trois autres hôpitaux britanniques ont été infectés par une variante du ver Mytob, lequel a obligé les établissements à déconnecter tous les ordinateurs pendant 24 heures pour résoudre l'incident.

En 2013, 200 ordinateurs du Cook County Department of Highway and Transportation ont été infectés. Ces systèmes étaient responsables de la maintenance de centaines de kilomètres d'autoroutes dans la région de Chicago. Suite à l'attaque, le réseau a dû être arrêté pendant neuf jours afin de désinfecter tous les ordinateurs.

Cette liste d'incidents montre que le danger des cyber-attaques menées contre les infrastructures critiques est réel et, à l'heure actuelle, toutes les autorités sont conscientes des risques que cela implique.

# Une protection avancée pour les infrastructures essentielles.

La réalité telle que nous l'avons constatée et avec laquelle nous vivons nous montre qu'il est nécessaire de contrôler la protection des infrastructures critiques afin d'assurer un plus haut niveau de protection contre ces menaces.

En mai 2016, à l'issue d'une réunion des ministres de l'énergie du G7, une déclaration commune a été publiée. Elle stipulait, entre autres, qu'il fallait insister sur l'importance de mettre en place des systèmes énergétiques robustes, qu'il s'agisse du gaz, de l'électricité et du pétrole, afin d'apporter une réponse efficace face aux cyber-menaces et d'assurer la continuité des services critiques.

**Pour améliorer la prévention et la réponse face à des attaques logiques, les gouvernements mettent en œuvre une série de mesures à l'échelle globale.** Ces mesures visent à installer des centres collectant toutes les informations

pertinentes pour l'amélioration de la protection des infrastructures critiques. Une stratégie complète a ainsi été élaborée en vue de s'attaquer au problème et cet aspect doit être inscrit dans les législations nationales.

La sécurité des infrastructures critiques est-elle à l'heure actuelle appropriée ? Il est difficile de répondre à cette question car les informations ou les techniques potentiellement utilisables par les cybercriminels sont inconnues, de sorte qu'il est impossible de garantir une sécurité à 100 %. Les pistes d'amélioration portent sur la protection contre les attaques connues, et celles-ci peuvent être évitées en adoptant, entre autres, les bonnes pratiques suivantes :

## Bonnes pratiques

- 1. Contrôle des systèmes à la recherche de vulnérabilités, en particulier les vulnérabilités avec failles de sécurité signalées et connues depuis un certain temps...**
- 2. Les réseaux servant à contrôler ces infrastructures doivent faire l'objet d'une surveillance adaptée et, le cas échéant, être isolés des connexions externes. Cela permettra la détection d'attaques externes et préviendra l'accès aux systèmes contrôlés à partir d'un réseau interne.**
- 3. Le contrôle des lecteurs amovibles est essentiel sur n'importe quelle infrastructure et pas seulement parce qu'ils ont constitué le vecteur d'attaques aussi notoires que celles du ver Stuxnet. Lors de la protection de telles infrastructures critiques, il est crucial de s'assurer que les logiciels malveillants n'entrent pas sur le réseau interne via des clés USB ou que celles-ci ne servent pas à dérober des informations confidentielles.**
- 4. La surveillance des PC auxquels des automates programmables industriels (API) sont connectés. Ces équipements connectés via Internet sont les plus sensibles car ils peuvent donner à un pirate l'accès à des systèmes de contrôle-commande critiques. Par ailleurs, même s'il ne parvient pas à prendre le contrôle d'un système, le cyber-criminel peut obtenir des informations précieuses pour d'autres vecteurs d'attaque.**

# La solution

La solution consiste à se prémunir contre les menaces sophistiquées et les attaques ciblées, y compris par une détection des comportements inhabituels ou suspects. Il faut un système capable de protéger la confidentialité des données et le caractère privé des informations, ainsi que les actifs et la réputation d'une entreprise.

Cette plate-forme intelligente sera en mesure d'aider le personnel chargé de la sécurité à réagir rapidement aux menaces sur les réseaux critiques et fera en sorte qu'il dispose des informations indispensables pour apporter une réponse adéquate.

**Cette solution existe et s'appelle Adaptive Defense 360. Ce système de cybersécurité de pointe est le seul à combiner une protection de dernière génération et une technologie de résolution capable de classer 100 % des processus en cours d'exécution.**

Adaptive Defense 360 assure la classification d'absolument tous les processus actifs sur les postes client, pour une protection garantie contre les logiciels malveillants connus et les attaques « zero-day », les menaces persistantes avancées et les attaques ciblées. La plate-forme fait appel à une logique contextuelle pour identifier des modèles de comportement malveillants et générer des actions de cybersécurité sophistiquées contre les menaces connues et inconnues.

Elle analyse, catégorise et corrèle les données collectées sur les cybermenaces, afin d'assurer des tâches de prévention, de détection, de réponse et de résolution.

Elle détermine les modes d'accès aux données et leurs utilisateurs, et contrôle les fuites de données, qu'elles soient le fait de logiciels malveillants ou d'employés indisciplinés.

Enfin, elle identifie et résout les vulnérabilités système et celles des programmes installés, et empêche l'utilisation d'applications indésirables (barres d'outils, logiciels publicitaires, modules complémentaires, etc.).



# Pour plus d'information :

## **BENELUX**

+32 15 45 12 80  
belgium@pandasecurity.com

## **BRAZIL**

+55 11 3054-1722  
brazil@pandasecurity.com

## **FRANCE**

+33 (0) 1 46842 000  
commercial@fr.pandasecurity.com

## **GERMANY (& AUSTRIA)**

+49 (0) 2065 961-0  
sales@de.pandasecurity.com

## **HUNGARY**

+36 1 224 03 16  
hungary@pandasecurity.com

## **ITALY**

+39 02 24 20 22 08  
italy@pandasecurity.com

## **MEXICO**

+52 55 8000 2381  
mexico@pandasecurity.com

## **NORWAY**

+47 93 409 300  
norway@pandasecurity.com

## **PORTUGAL**

+351 210 414 400  
geral@pt.pandasecurity.com

## **SOUTH AFRICA**

+27 21 683 3899  
sales@za.pandasecurity.com

## **SPAIN**

+34 900 90 70 80  
comercialpanda@pandasecurity.com

## **SWEDEN (FINLAND & DENMARK)**

+46 0850 553 200  
sweden@pandasecurity.com

## **SWITZERLAND**

+41 22 994 89 40  
info@ch.pandasecurity.com

## **UNITED KINGDOM**

+44(0) 800 368 9158  
sales@uk.pandasecurity.com

## **USA (& CANADA)**

+1 877 263 3881  
sales@us.pandasecurity.com

Plus d'information sur :  
[pandasecurity.com/enterprise/solutions/adaptive-defense-360/](https://pandasecurity.com/enterprise/solutions/adaptive-defense-360/)

pour obtenir gratuitement votre version d'évaluation, appelez-nous :

**01 46 84 20 00**

ou par email : [democloud@fr.pandasecurity.com](mailto:democloud@fr.pandasecurity.com)





# Adaptive Defense 360

**Visibilité sans limite, contrôle absolu**