CERT.be

POUR LA SÉCURITÉ INTERNET ET RÉSEAU DE VOTRE ORGANISATION

CYBERINCIDENTS
Résolution et prévention


CERT.be
The Federal Cyber Emergency Team

Cybercriminalité : les risques pour votre entreprise

La cybercriminalité aujourd'hui

Comment CERT.be peut-il aider votre organisation ?

Témoignages

Informations pratiques

Cybercriminalité : les risques pour votre entreprise

« Il faut nous voir comme les pompiers, pas comme la police. Nous ne sanctionnons pas, mais assurons une coordination pour éteindre l'incendie au plus vite. Et nous travaillons avec discrétion, en toute confiance. »

Christian Van Heurck,
coordinateur de CERT.be

Avec des auteurs de plus en plus professionnels la criminalité sur Internet est en pleine expansion. **Votre organisation peut aussi en être victime**. Et lorsque plusieurs entreprises subissent une attaque collective, c'est même l'économie nationale qui est en péril. Une telle éventualité doit absolument être évitée. En tant qu'expert en sécurité Internet et réseau, CERT.be entend aider votre entreprise, ainsi que d'autres organisations, à **coordonner, résoudre et prévenir les problèmes de sécurité**.

Quelles sont les tâches de CERT.be ?

- **Rassembler et fournir des informations** sur les incidents de sécurité
- **Apporter un soutien** en cas d'incident
- **Coordonner la gestion d'incidents** à grande échelle
- Contribuer à la **mise en place d'activités CERT** au sein de votre entreprise
- **Partager des données et connaissances** par le biais de publications et d'événements

Résoudre les problèmes…

CERT.be est la cyber emergency team (l'équipe d'intervention d'urgence en sécurité informatique) fédérale. Nous sommes une organisation neutre et non commerciale, reconnue par un réseau international d'experts en sécurité. En cas d'incident de sécurité dans votre organisation, vous pouvez nous le signaler en toute discrétion. Comme nous collectons et analysons en permanence des informations sur les incidents de sécurité, nous pouvons dépister plus aisément et plus rapidement l'origine d'un problème. Nous disposons également d'experts susceptibles de vous épauler dans la résolution d'un grave incident de sécurité.

… et les prévenir

Votre organisation est et reste naturellement responsable de la protection de vos ordinateurs et réseaux. Mais CERT.be vous apporte son soutien, surtout en vous informant sur les menaces et les solutions permettant de maintenir les risques sous contrôle.

La cyber-criminalité **aujourd'hui**

Actuellement, la cybercriminalité est une **réalité quotidienne**. Si votre organisation n'y a pas encore été confrontée, elle court un risque réel de l'être à l'avenir. Depuis longtemps déjà, les criminels ne dirigent plus leurs flèches uniquement vers des secteurs critiques tels que les banques. **Les entreprises « ordinaires » ou d'autres organisations se retrouvent, elles aussi, de plus en plus souvent dans leur collimateur**. La nature internationale d'Internet fait que les menaces peuvent venir de partout.

En phase avec les dernières tendances

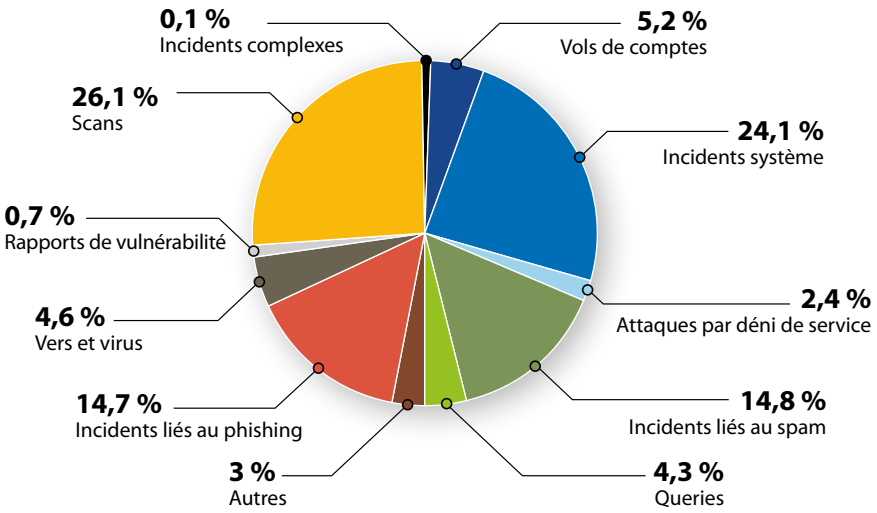
Les cybercriminels suivent les tendances : ainsi, la diffusion de virus via l'e-mail demeure importante, mais les risques de contamination au travers des sites de réseaux sociaux et des apps augmentent. Si chaque collaborateur de votre entreprise ou organisation peut télécharger et utiliser n'importe quelle application via un smartphone ou une tablette, vous courez un risque accru. Vous n'êtes pas obligé de bannir ces appareils du lieu de travail, mais il vaut mieux adapter votre modèle de sécurité à la nouvelle situation. Les informations et analyses de CERT.be vous aideront à évaluer correctement les dangers.

Professionnalisme à grande échelle

Le danger principal ne vient plus de hackers individuels, mais bien de bandes organisées qui négocient les données personnelles, secrets d'entreprises et logiciels malveillants sur le marché noir. Ces groupes lancent des attaques ciblées sur des entreprises et organisations, mais contrairement aux hackers individuels, ils tiennent essentiellement à rester invisibles. Le système de votre entreprise peut donc être infiltré à votre insu. Les publications et réunions de CERT.be sensibilisent les experts IT aux problèmes.

“Les informations et analyses de CERT.be vous aideront à évaluer correctement les dangers.”

Incidents de sécurité en **Belgique**



En 2011, 2.609 incidents de sécurité, dont 1.161 incidents graves, ont été rapportés à CERT.be. Un incident grave est un cas de fraude, une tentative de fraude ou une usurpation d'identité dans le secteur bancaire, une attaque par déni de service ou une grave infection par un virus. CERT.be a lancé 1.494 enquêtes à la suite des notifications reçues.

Un faible niveau de sensibilisation en matière de sécurité

Le faible niveau de sensibilisation chez les utilisateurs finaux accroît les risques. Ainsi, les collaborateurs compromettent régulièrement la sécurité des systèmes IT sans s'en rendre compte, par exemple en travaillant sur un appareil non protégé, en communiquant un mot de passe en toute bonne foi, en réutilisant des mots de passe faibles ou en cliquant sur un lien dans un e-mail de phishing. Les utilisateurs qui travaillent sans logiciels de protection ou avec des versions obsolètes peuvent également causer des problèmes à votre entreprise. Voilà pourquoi CERT.be s'adresse aussi aux utilisateurs individuels, pour lesquels il établit des campagnes de sensibilisation.

L'arsenal gagne en puissance

Les malwares ou logiciels malveillants utilisés par les criminels sont de plus en plus difficiles à neutraliser. Certains possèdent même leur propre mécanisme de défense. CERT.be rassemble automatiquement des informations sur les menaces et incidents par le biais de capteurs, de honeypots (des systèmes de leurre) et d'autres systèmes.

Nous collectons aussi les informations qui nous sont communiquées par d'autres cyber emergency teams, des organisations et des entreprises.

Formes fréquentes de **cybercriminalité**

Botnets

Les botnets sont des réseaux d'ordinateurs infectés qui transmettent du spam en masse, propagent des virus, envoient des données cachées et attaquent des systèmes informatiques.

Distributed denial of service (DDoS) attack (attaque par déni de service)

Une "DDoS attack" est un type d'attaque perpétré par un botnet. Pilotés par un centre de commande, un grand nombre d'ordinateurs infectés se connectent simultanément à un serveur (Web) d'une entreprise. Celui-ci devient dès lors temporairement indisponible ou il plante.

Advanced persistent threats (menaces persistantes avancées)

Les criminels tentent de pénétrer subrepticement dans des systèmes d'entreprises et d'y rester le plus longtemps possible pour voler un maximum d'éléments : droits de propriété intellectuelle, secrets d'entreprise, informations sur des processus internes…

Malware (logiciels malveillants)

Un cheval de Troie, par exemple, se présente sous la forme d'un programme ordinaire, d'une vidéo, d'un jeu ou d'une autre application, mais il contamine un ordinateur à l'insu de son utilisateur. Les chevaux de Troie sont utilisés pour collecter des mots de passe, des logins et des adresses e-mail, voire pour prélever de l'argent sur des comptes bancaires. Un ver exploite les failles dans la sécurité d'un réseau pour se propager d'un ordinateur à l'autre. Il utilise alors les appareils infectés pour voler des données, envoyer du spam, lancer des attaques DDoS ou mener d'autres activités criminelles.

Social engineering et phishing

Les criminels ne se contentent pas d'exploiter les points faibles de la technologie : ils s'orientent aussi vers l'individu. Ils essaient de voler des informations confidentielles ou secrètes en mystifiant des utilisateurs d'ordinateurs. Les e-mails et sites Web de phishing qui demandent au destinataire de communiquer ses numéros de carte de crédit ou ses mots de passe en sont un exemple. Il s'agit parfois de fidèles reproductions de véritables e-mails ou sites Web. Les informations obtenues, comme les mots de passe, peuvent alors être utilisées pour se connecter sur vos systèmes d'entreprise.

De plus en plus **organisés**

La **nature**, le **nombre** et l'**ampleur** des activités cybercriminelles ont considérablement évolué ces dernières années.

1988 – Le premier ver informatique

Le premier ver informatique, Morris, se propage via Internet. Il donne lieu à la création de la première cyber emergency team aux États-Unis.

2000 – Virus agressifs

Les virus agressifs occasionnent d'énormes préjudices à l'échelle mondiale. Le trafic réseau de certaines entreprises est paralysé par une saturation. Parmi les virus les plus connus figurent ILOVEYOU (2000) et Sasser (2004). ILOVEYOU est envoyé en pièce jointe à des e-mails et contamine des millions d'ordinateurs du monde entier en quelques heures.

2004 – Les botnets attaquent

Des botnets attaquent des entreprises. En 2004, une agence britannique de paris en ligne est victime de chantage et refuse de payer. Elle fait alors l'objet d'une attaque par déni de service : un botnet – un réseau d'ordinateurs infectés – envoie une énorme masse de données vers son site Web, qui se retrouve paralysé.

2007 – Attaques par déni de service

Des cyberterroristes mènent des attaques par déni de service contre les autorités. En 2007, des botnets attaquent les infrastructures critiques d'Estonie. Ils ciblent le secteur de l'énergie, les banques, les services publics et les transports. Le gouvernement décide de suspendre tout trafic de données avec l'étranger.

2010 – Cyberespionnage et cyberguerres

Le ver Stuxnet dérègle les installations d'enrichissement de l'uranium en Iran. Ce malware attaque le logiciel d'exploitation de systèmes industriels et peut ainsi saboter des entreprises et immobiliser, voire commander leurs infrastructures critiques. Le Pentagone a affirmé en 2011 qu'une cyberattaque d'une puissance étrangère pourrait désormais être considérée comme une déclaration de guerre.

2012 – Collaboration contre la cybercriminalité

Les cyber emergency teams, les entreprises privées et la police interviennent parfois ensemble, par exemple lors de la lutte contre le virus DNSChanger. Ce virus contamine 4 millions d'ordinateurs dans le monde entier afin de les détourner vers de faux sites Web ou des sites publicitaires. Le FBI américain arrête les créateurs du virus avec l'aide du secteur privé. Les différentes cyber emergency teams, dont CERT.be, organisent des campagnes.

... – Hacktivistes

Les hacktivistes recourent de plus en plus souvent aux attaques par déni de service pour susciter l'attention des médias et occasionner des dommages. L'une des organisations hacktivistes les plus connues, Anonymous, a paralysé les sites Web de diverses entreprises car elle les soupçonnait d'actions à l'encontre de Wikileaks.

Comment CERT.be peut-il aider votre entreprise ?

Une protection efficace de vos ordinateurs et réseaux est essentielle au bon fonctionnement de votre entreprise. CERT.be possède **l'expérience et les connaissances requises** pour vous y aider. Nos tâches principales sont la **coordination**, la **prévention** et **l'information**.

Prévenir les problèmes

Nos services proactifs sont axés sur la prévention des cyber-incidents et la limitation de leur impact, le cas échéant. Dans le moyen et le long terme, nous nous efforçons d'améliorer la protection des infrastructures IT par divers biais :

- **publication d'informations** et de **conseils** sur la protection
- suivi et évaluation des **tendances** et **technologies**
- **sensibilisation** des spécialistes et utilisateurs de systèmes IT
- **partage de connaissances et d'informations**
- organisation de **conférences** et **d'ateliers spécialisés**.

Résoudre les problèmes

Nos services réactifs soutiennent votre entreprise pour une résolution rapide et efficace des incidents de sécurité. Pour ce faire, nous recourons aux méthodes suivantes :

- **coordination** et **conseils relatifs** à la gestion des incidents
- **évaluation des menaces**
- **publication d'alertes et d'avertissements** sur www.cert.be, Twitter et via RSS
- **publication de conseils et de rapports**
- soutien ou coordination de la **gestion d'incidents**.

CERT.be – un **réseau** de spécialistes à votre disposition

1 • Proactif

Vous n'avez peut-être pas remarqué l'attaque dirigée contre vous ; nous en sommes au courant avant vous. S'il s'agit d'un incident grave, nous vous en avertissons.

2 • À votre initiative

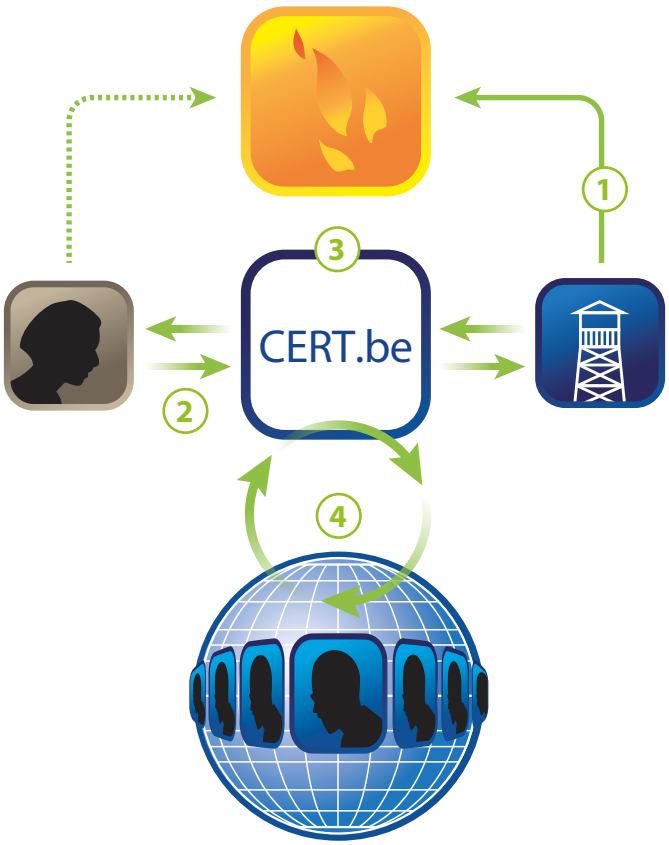
Vous êtes ou pensez être victime d'un cyberincident. Vous en informez CERT.be.

3 • Consultation interne

Notre spécialiste évalue la gravité de la situation. Il consulte ses contacts en interne et nous vous informons de ses conclusions.

4 • Autres spécialistes

En cas d'incident grave, nous nous adressons à nos autres canaux. Par le biais d'une collaboration intense et d'un échange d'informations suivi avec notre réseau de spécialistes extérieurs, dont les membres d'autres CERT, nous tentons d'éliminer au plus vite le problème.



Gestion de la protection

Nos services de management visent une gestion optimale de la protection. Nous mettons donc notre expertise à la disposition d'entreprises et d'organisations désireuses de lancer leurs propres activités CERT. La création d'une cyber emergency team au sein de votre entreprise facilite la communication entre CERT.be et vous, mais aussi entre vous et les cyber emergency teams d'autres organisations.

Une telle communication est extrêmement utile, car les incidents dépassent souvent le cadre d'une entreprise. Les cyber emergency teams peuvent partager en toute discrétion les conseils et expériences qui les aideront à gérer et traiter les incidents avec un maximum d'efficacité.

Collaboration internationale

Comme les menaces posées aux réseaux viennent souvent d'autres pays, CERT.be déploie ses activités dans un réseau mondial d'experts en cyberprotection. Si votre entreprise constate une attaque électronique, un hacking ou une tentative d'effraction et nous en avertit, nous prenons contact avec nos collègues étrangers afin d'identifier l'origine des problèmes. La collaboration internationale se manifeste au travers d'un réseau d'experts en cyberprotection qui se connaissent personnellement, et l'échange d'informations s'effectue en toute discrétion, sans communication de données sur les entreprises concernées.

Comme les menaces posées aux réseaux viennent souvent d'autres pays, CERT.be déploie ses activités dans un réseau mondial d'experts en cyberprotection.

Traffic Light Protocol (TLP)

À l'instar d'autres cyber emergency teams, CERT.be recourt au protocole TLP (Traffic Light Protocol) pour assurer et encourager un échange d'informations sécurisé.

- **Rouge** – Informations exclusivement réservées aux destinataires directs
- **Orange** – Informations destinées à une entreprise, éventuellement limitées à certains de ses collaborateurs
- **Vert** – Informations destinées à une communauté, à ne pas diffuser sur Internet
- **Blanc** – Informations librement diffusables, pour autant que cette démarche ne soit pas contraire à la loi (par exemple la loi sur le droit d'auteur).

Que peut faire votre entreprise par elle-même ?

- ✓ **Soyez proactifs.** Dressez l'inventaire de vos points faibles (vulnerability management) et déterminez comment vous allez y remédier en assurant l'amélioration et la tenue à jour des systèmes et logiciels (patch management).
- ✓ **Utilisez des logiciels et dispositifs sécurisés** tels que des pare-feu.
- ✓ N'attendez pas tout d'une seule technologie. **Combinez les solutions**.
- ✓ Tenez compte du **facteur humain**. Les initiatives de sensibilisation sont essentielles pour attirer l'attention des collaborateurs sur la problématique de la sécurité. Combinez cette sensibilisation avec une charte spécifiant ce que les collaborateurs peuvent faire ou non.
- ✓ **N'exagérez pas avec les interdictions**. Une politique trop stricte en matière de sécurité peut inciter le personnel à contourner les règles avec leurs propres dispositifs tels que des smartphones et des tablettes.
- ✓ Envisagez de lancer **vos propres activités CERT** avec un responsable de la sécurité IT. Disposer d'un contact interne reconnu qui maîtrise la problématique de la sécurité et auquel d'autres spécialistes peuvent parler en toute confiance est extrêmement important.
- ✓ Établissez une politique des **mots de passe** et donnez des conseils à vos collaborateurs pour utiliser des mots de passe sûrs et différents.
- ✓ **Soyez préparé :** vous pouvez à tout moment être victime d'une attaque. Sachez comment réagir en cas d'incident. Gardez des back-ups testés ainsi que vos systèmes de connexion et de contrôle à pied d'œuvre, afin de pouvoir détecter et résoudre rapidement les problèmes éventuels.

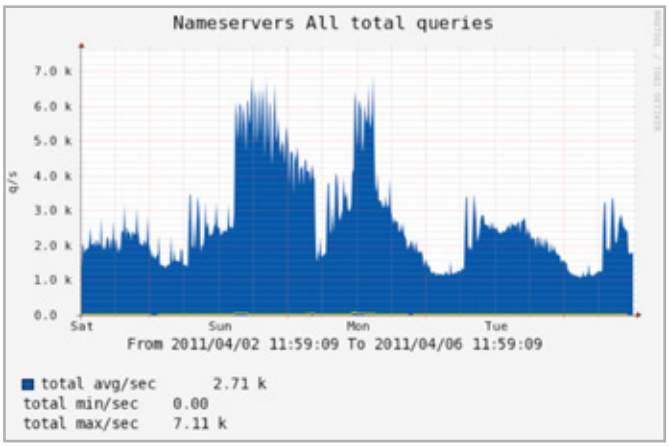
Les entreprises **témoignent**

Bien qu'elle ne date pas d'hier la cybercriminalité revêt aujourd'hui d'autres formes, souvent **très structurées**. Les organisations et entreprises qui en ont été victimes mettent tout en œuvre pour ne plus y être confrontées. **Leur ouverture permet** à CERT.be de contribuer à **prévenir** ou **résoudre** de graves incidents. Les organisations mentionnées aux pages suivantes ont fait appel aux services de CERT.be

“La communication ouverte et le partage d’informations revêtent une grande importance”

Philip Du Bois
General Manager de DNS.be

« Début avril 2011, nos serveurs ont subitement reçu six fois plus de requêtes (‘queries’) à traiter que d’habitude.
Ce surcroît d’activité était imputable à un réseau d’ordinateurs piratés tentant d’abuser des serveurs mail de noms de domaine .be. Une attaque inutile car nous n’enregistrons aucune donnée de serveurs mail sur nos noms de domaine.



Nous avons remarqué le trafic suspect car nous contrôlons la nature des demandes, l’utilisation de la bande passante et le statut de nos serveurs de noms via un système de monitoring. Nous avons averti CERT.be, qui a lancé une analyse sur la base des données de l’incident collectées par nos soins. Cette communication ouverte et le partage d’informations revêtent une grande importance. Ils renforcent également l’expertise interne.

En définitive, tout le monde peut être victime d’une cyberattaque même s’il est extrêmement bien protégé. Voilà pourquoi je recommande d’être proactif : contactez à l’avance les spécialistes de CERT.be. Leur numéro est comme celui des pompiers ou de l’hôpital. Il doit être à portée de main dans votre équipe IT. »

DNS.be gère 1,25 million de noms de domaine .be, et a récemment été autorisée par les instances flamandes et bruxelloises à gérer les nouvelles extensions .vlaanderen et .brussels.

La sécurité informatique n'est pas un luxe

Simon François
Responsable réseau et sécurité à l'ULg

« En 2010, l'Université a subi une attaque de type DoS (Denial of Service) visant un des serveurs du pôle de biotechnologie. Cette attaque consistait en **l'envoi massif de millions de paquets DNS illégitimes**, à raison de 1,5 Gbit/s, ce qui a eu pour conséquence de neutraliser nos deux lignes de pare-feu périmétriques et de priver l'Université de son accès Internet.

Ce problème a **rapidement été diagnostiqué par nos ingénieurs sécurité** et nous avons immédiatement sollicité l'aide du CERT.be. Après une rapide analyse, CERT.be est intervenu au niveau des routeurs de Belnet (le réseau national de la recherche) afin de rediriger le trafic réseau malveillant vers un **trou noir en amont de l'ULg**.

Il convient de rappeler que les cyberattaques sont légion et ne touchent pas que les autres ; nous avons pu constater que le CERT.be est à l'écoute de tous pour apporter une réponse efficace. »

La fondation de l'Université de Liège remonte à 1817. Aujourd'hui forte de 5.000 emplois directs, dont 3.300 enseignants et chercheurs, l'ULg a tissé un réseau de relations avec plus de 600 institutions, faisant de l'ouverture au monde une de ses priorités.

www.ulg.ac.be

“CERT.be: le lien vers l’expertise étrangère”

Paul Boons
Agfa Information Security Officer

“Chez Agfa, nous menons une politique proactive en matière de sécurité. L’échange d’informations joue un rôle crucial sur ce plan et il est important que cela s’effectue à l’échelon international. D’abord parce qu’Agfa mène des activités internationales qui englobent notre réseau de données. Ensuite parce que la cybercriminalité **se joue des frontières**. C’est donc quasi naturellement que nous sommes arrivés chez CERT.be.

CERT.be fait partie d’un réseau professionnel international. Une couverture utile en cas de cybermenace mais aussi une importante valeur ajoutée sur le plan préventif. Ils sont souvent très vite au courant de menaces concrètes et peuvent nous **fournir des informations pertinentes** pour prévenir ou enrayer une cybermenace grâce aux contacts qu’ils entretiennent avec leurs collègues internationaux.

CERT.be organise aussi des **séminaires réguliers sur la cybercriminalité**. Nous envoyons volontiers nos collaborateurs à ces points de rencontre internationaux : c’est l’idéal pour rester à jour et partager des informations avec des collègues d’autres entreprises.

En ce qui me concerne, CERT.be a un rôle important à jouer dans l’échange d’informations techniques avec les entreprises. Lorsque nous identifions des modèles techniques, nous pouvons vérifier auprès de CERT.be s’ils existent aussi dans d’autres entreprises. **L’échange de ces spécifications**, anonymement ou non via CERT.be, peut contribuer à une protection efficace des réseaux d’entreprises.”

Leader mondial en matière d’imagerie, Agfa développe, produit et distribue des produits et systèmes analogiques et numériques permettant de créer, traiter et reproduire des images. Elle est surtout connue pour ses solutions dans les secteurs graphique et médical. Le siège central d’Agfa se situe à Mortsel près d’Anvers. L’entreprise produit aussi aux États-Unis, en Allemagne et en Chine, et possède des bureaux de vente dans plus de 40 pays. Le département Agfa ICS (Information & Communication Services) emploie 460 personnes dans le monde entier et assure la gestion ainsi que la protection des connexions réseau entre 100 emplacements. Agfa ICS est également responsable des centres de données d’Agfa, notamment en Belgique, en Allemagne et au Canada.

Informations **pratiques**

Point de contact **central**

CERT.be est le point de contact central pour les problèmes liés à la cybersécurité. Vous pouvez nous soumettre gratuitement vos questions sur la protection et la gestion des risques.

Questions générales

Par e-mail à info@cert.be
Par téléphone au 02 790 33 33,
les jours ouvrables de 9 à 17 heures

Signaler des incidents de sécurité

Par e-mail à cert@cert.be
Vous pouvez crypter les informations confidentielles à l'aide de notre clé publique. Vous trouverez de plus amples informations à ce sujet sur www.cert.be
Par téléphone au 02 790 33 85

Lorsque vous signalez un cyberincident

Communiquez toujours vos données de contact complètes et répondez le plus exhaustivement possible aux questions suivantes :

- ✓ Quand l'incident a-t-il débuté ?
- ✓ Qui en avez-vous déjà informé ?
- ✓ De quel type d'incident s'agit-il : DDoS, malware… ?
- ✓ L'incident est-il toujours en cours ? Comment se manifeste-t-il ?
- ✓ Quel est l'impact de l'incident ?
- ✓ Avez-vous déjà pris des mesures ?
- ✓ Disposez-vous de journaux « logs » ou d'autres données utiles ?
- ✓ Qu'attendez-vous de votre notification ?
- ✓ Souhaitez-vous déclarer l'incident à la police ?

Qui contribue
à CERT.be ?

CERT.be est la cyber emergency team fédérale, fondée en 2009 et exploitée par Belnet, le réseau national belge de la recherche, à la demande de Fedict.

Belnet gère le réseau de recherche pour les universités, écoles supérieures, centres de recherche et services publics belges.

Belnet a très vite établi son propre CERT afin de surveiller son réseau et d'informer ses clients. Avant la fondation de CERT.be, le CERT de Belnet était de facto le point de contact international pour tout ce qui a trait à la protection des réseaux belges.

Fedict (Service public fédéral Technologie de l'information et de la communication) œuvre à la mise en place de l'e-gouvernment et aide les services publics fédéraux à améliorer leurs relations avec les citoyens, entreprises et fonctionnaires via l'ICT.

Fedict est à la base de nombreux projets technologiques innovants tels que Tax-on-web, le point de contact eCops et la carte d'identité électronique.

Signalez vos cyberincidents en toute discrétion

Vous n'êtes peut-être pas les seuls à être attaqués…
D'autres ont peut-être déjà trouvé une solution…
Votre solution peut aider d'autres victimes…

cert@cert.be

02 790 33 85

CERT.be
The Federal Cyber Emergency Team

Belnet – CERT.be
Avenue Louise 231
1050 Bruxelles

www.cert.be
info@cert.be
Tél. : 02-790 33 33

Éditeur responsable : Belnet, Jan Torreele, Avenue Louise 231, 1050 Bruxelles

Cypres