

CEART.be

VOOR MEER INTERNET- EN NETWERKVEILIGHEID IN UW ORGANISATIE



CYBERINCIDENTEN
oplossen & voorkomen





Cybercrime, ook uw bedrijf loopt gevaar



04



06

Cybercrime vandaag



10

Hoe kan CERT.be
uw organisatie helpen?



14

Bedrijven getuigen



16

Praktische informatie



Cybercrime, ook uw bedrijf loopt gevaar

“

Je moet ons zien als de brandweer, niet de politie. Wij bestraffen niet, maar coördineren om zo snel mogelijk de brand te blussen. En wij werken in alle vertrouwen en in alle discretie.

Christian Van Heurck,
coördinator CERT.be

”

Het aantal misdaden op het internet stijgt. Criminelen gaan steeds professioneler te werk. **Ook uw organisatie kan een slachtoffer worden.** Als vele bedrijven samen door een grote aanval in moeilijkheden raken, loopt zelfs de nationale economie gevaar. Zover mag het niet komen. Als specialist in internet- en netwerkveiligheid wil CERT.be uw bedrijf en andere organisaties helpen bij **het coördineren, oplossen en voorkomen van veiligheidsproblemen.**



Wat doet CERT.be?

- **Informatie verzamelen** en **geven** over veiligheidsincidenten
- **Ondersteuning bieden** wanneer incidenten zich voordoen
- De behandeling van grootschalige **incidenten coördineren**
- Helpen bij het **opzetten van CERT-activiteiten** in uw eigen bedrijf
- **Gegevens en kennis delen** via publicaties en events

Problemen oplossen...

CERT.be is het federale cyber emergency team. Wij zijn een neutrale, niet-commerciële organisatie, erkend door een internationaal netwerk van beveiligingsexperten. Als er zich in uw organisatie een veiligheidsincident voordoet, kunt u dat in alle discretie aan ons melden. Omdat wij permanent informatie over veiligheidsincidenten verzamelen en analyseren, kunnen wij makkelijker en sneller de oorsprong van een probleem achterhalen. Ook hebben wij experts die u kunnen ondersteunen bij de oplossing van een ernstig veiligheidsincident.

... en voorkomen

Uw organisatie is en blijft natuurlijk zelf verantwoordelijk voor de beveiliging van haar computers en netwerken. Maar CERT.be ondersteunt u, in de eerste plaats door u te informeren over bedreigingen en over manieren om de risico's onder controle te houden.

Cybercrime vandaag

Cybercriminaliteit is een **dagelijkse realiteit**. Als uw organisatie er nog niet mee te maken kreeg, is de kans reëel dat ze er in de toekomst wel mee wordt geconfronteerd. Criminelen richten hun pijlen al lang niet meer enkel op kritische sectoren zoals banken.

Ook **'gewone' bedrijven of andere organisaties zijn steeds meer een doelwit**. Het grensoverschrijdend karakter van internet maakt dat de bedreigingen van overal kunnen komen.

Mee met de nieuwste trends

Cybercriminelen volgen de trends: de verspreiding van virussen via e-mail blijft bijvoorbeeld belangrijk, maar de risico's op besmetting via sociale netwerksites en apps nemen toe. Als elke werknemer eender welke applicatie in uw bedrijf of organisatie via een smartphone of tablet kan downloaden en gebruiken, loopt u een verhoogd risico. U hoeft deze toestellen niet te bannen van de werkvloer, maar u past uw veiligheidsmodel wel het best aan de nieuwe situatie aan. De informatie en analyses van CERT.be helpen u de gevaren correct in te schatten.

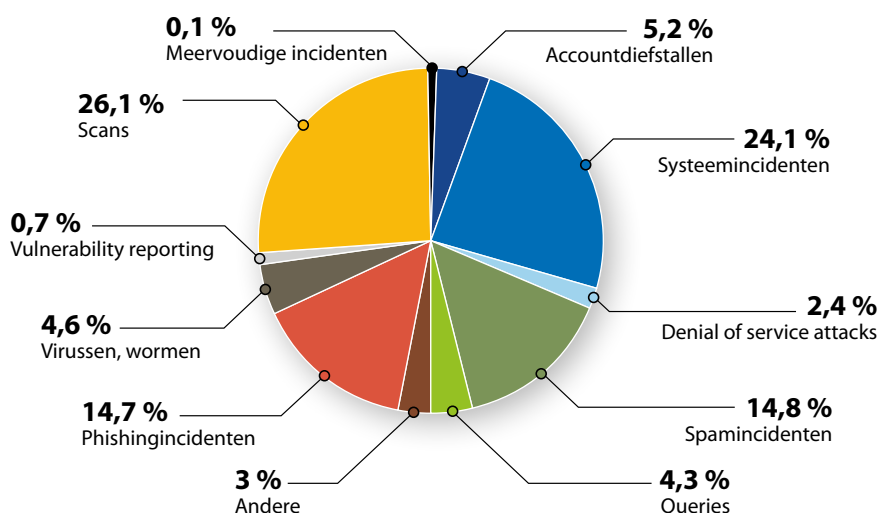


Professioneel en grootschalig

Het grootste gevaar komt niet meer van individuele hackers maar van georganiseerde bendes die persoonlijke gegevens, bedrijfsgeheimen en malware op de zwarte markt verhandelen. Zij voeren doelgerichte aanvallen uit op bedrijven en organisaties. In tegenstelling tot individuele hackers wil de georganiseerde criminaliteit vooral onzichtbaar blijven. Uw bedrijfssysteem kan geïnfiltreerd zijn, zonder dat u het beseft. In publicaties en op bijeenkomsten maakt CERT.be IT-specialisten bewust van de problemen.

“
De informatie
en analyses
van CERT.be
helpen u de
gevaaren correct
in te schatten.
”

Veiligheidsincidenten in België



In 2011 werden bij CERT.be 2.609 veiligheidsincidenten gerapporteerd, waaronder 1.161 ernstige incidenten. Een ernstig incident is een geval van fraude, een poging tot fraude of identiteitsdiefstal in de banksector, een denial of service attack of een ernstige virusuitbraak. CERT.be startte 1.494 onderzoeken naar aanleiding van de meldingen.

Laag veiligheidsbewustzijn

Het lage veiligheidsbewustzijn bij eindgebruikers verhoogt de risico's. Werknemers brengen geregeld, zonder het te beseffen, de veiligheid van IT-systemen in gevaar, bijvoorbeeld door op een onbeveiligd toestel te werken, een wachtwoord te goeder trouw door te geven, zwakke wachtwoorden te hergebruiken of een link in een phishingmail aan te klikken. Ook gebruikers die zonder of met verouderde beveiligings- en andere software werken, kunnen uw bedrijf in moeilijkheden brengen. Daarom richt CERT.be zich ook tot individuele gebruikers en zetten we bewustmakingscampagnes op.

Arsenaal wordt krachtiger

De malware of kwaadaardige software die criminelen gebruiken, wordt alsmaar moeilijker uit te schakelen. Sommige malware heeft zijn eigen verdedigingsmechanisme aan boord. CERT.be verzamelt informatie over bedreigingen en incidenten op een automatische manier via sensors, honeypots (loksystemen) en andere systemen.

We brengen ook informatie samen die ons gemeld wordt door andere cyber emergency teams, organisaties en bedrijven.

Veel voorkomende vormen van cybercriminaliteit

Botnets

Botnets zijn netwerken van besmette computers die massaal spam versturen, virussen verspreiden, ongemerkt data doorsturen en aanvallen op computersystemen uitvoeren.

Distributed denial of service (DDoS) attack

Een DDoS attack is een bepaald type aanval van een botnet. Een groot aantal besmette computers maakt, aangestuurd door een centraal commandopunt, gelijktijdig een verbinding met een (web)server van een bedrijf. Daardoor wordt hij tijdelijk niet meer beschikbaar of crasht hij.

Advanced persistent threats

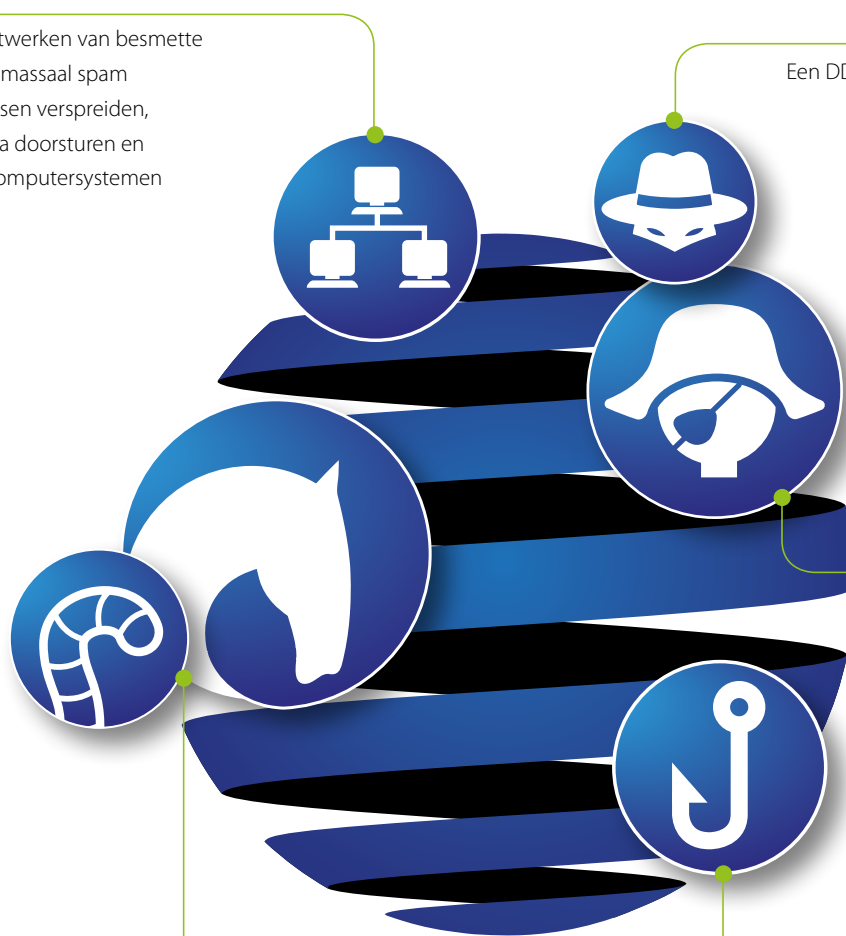
Criminelen proberen bedrijfs-systemen ongemerkt binnen te dringen en daar zolang mogelijk te blijven om zoveel mogelijk te stelen: intellectuele eigendomsrechten, bedrijfsgeheimen, informatie over interne processen, ...

Malware

Een Trojaans paard, bijvoorbeeld, wordt aangeboden als een gewoon programma, videofilmje, spelletje of een andere toepassing, maar het besmet de computer van de nietsvermoedende gebruiker. Trojaanse paarden worden gebruikt om wachtwoorden, logins en e-mailadressen te verzamelen, en soms ook om ongemerkt geld van bankrekeningen te halen. Een worm gebruikt gaten in de beveiliging van een netwerk om zich van de ene computer naar de andere computer te verspreiden. Hij gebruikt de geïnfecteerde toestellen om data te stelen, spam te versturen, DDoS-aanvallen uit te voeren of voor andere criminele activiteiten.

Social engineering en phishing

Criminelen proberen niet alleen kwetsbaarheden in de technologie uit te buiten, maar richten zich ook op de mens. Ze proberen vertrouwelijke of geheime informatie te stelen door computergebruikers te misleiden. Phishingmails en -websites die de ontvanger om kredietkaartnummers of wachtwoorden vragen, zijn een voorbeeld. Het zijn soms getrouwe kopieën van echte mails of websites. Verkregen informatie, zoals wachtwoorden, kan gebruikt worden om op uw bedrijfssystemen in te loggen.



Steeds meer georganiseerd

De **aard**, het **aantal** en de **schaal** van cybercriminele activiteiten zijn de voorbije jaren grondig veranderd.

De eerste computerworm 1988

De eerste computerworm, Morris, verspreidt zich via het internet. Het is de aanleiding tot de oprichting van het eerste cyber emergency team in de Verenigde Staten.

2000 Kwaadaardige virussen

Kwaadaardige virussen richten wereldwijd enorme schade aan. In bedrijven valt het netwerkverkeer soms stil door overbelasting. Bij de bekendste virussen zijn het ILOVEYOU-virus (2000) en Sasser (2004). ILOVEYOU wordt als bijlage bij e-mails verstuurd en besmet binnen enkele uren wereldwijd miljoenen computers.

Botnets vallen aan 2004

Botnets vallen bedrijven aan. In 2004 wordt een Brits online gokkantoor slachtoffer van afpersing. Omdat het bedrijf niet wil betalen, krijgt het af te rekenen met een denial of service attack. Via een botnet, een netwerk van besmette computers, wordt massaal veel data naar de website verstuurd, waardoor deze volledig lam komt te liggen.

2007 Denial of service attacks

Cyberterroristen voeren denial of service attacks uit op overheden. In 2007 vallen botnets de kritische infrastructuren van Estland aan. Ze richten zich op de energie-, bank-, overheids- en transportsector van het land. De regering besluit om alle dataverkeer met het buitenland af te sluiten.

Cyberspionage en -oorlog 2010

De Stuxnetworm ontregelt in Iran de installaties voor het verrijken van uranium. Deze malware valt besturingssoftware van industriële systemen aan en kan zo bedrijven saboteren, bedrijfskritische infrastructuur immobiliseren en overnemen. Het Pentagon verklaart in 2011 dat een cyberaanval vanuit een vreemde mogendheid voortaan als een oorlogsverklaring kan beschouwd worden.

2012 Samenwerking tegen cybercrime

Cyber emergency teams, privébedrijven en politie treden soms samen op, bijvoorbeeld bij de strijd tegen het DNSChanger-virus. Het virus besmet wereldwijd 4 miljoen computers en leidt computergebruikers om naar vervalste websites of naar sites met advertenties. De Amerikaanse FBI pakt met hulp van de privésector de bende achter het virus op. De diverse cyber emergency teams, zoals CERT.be, zetten campagnes op.

Hacktivisten ...

Hacktivisten gebruiken alsmear meer denial of service attacks om media-aandacht te genereren en schade aan te richten. Een van de meeste bekende hacktivistische organisaties, Anonymous, legde de websites van een aantal bedrijven plat, omdat ze verdacht werden van acties ten nadele van Wikileaks.

Hoe kan CERT.be uw bedrijf helpen?

Voor de goede werking van uw organisatie is een efficiënte internet- en netwerkbeveiliging essentieel. CERT.be heeft de **ervaring en de kennis** om u daarbij te helpen. Onze kerntaken zijn **coördinatie, preventie** en het **leveren van informatie**.

Problemen voorkomen

Onze proactieve diensten zijn gericht op het voorkomen van cyberincidenten en op het beperken van hun impact, als ze zich toch voordoen. Op middellange en lange termijn proberen we de beveiliging van IT-infrastructuren te verbeteren door:

- **informatie en adviezen te publiceren** over beveiliging
- **trends en technologieën** te volgen en te evalueren
- **bewustwording te creëren** bij IT-specialisten en gebruikers
- **kennis en informatie te delen**
- **conferenties** en gespecialiseerde **workshops** te organiseren.

Problemen oplossen

Onze reactieve diensten ondersteunen uw bedrijf bij het snel en effectief oplossen van veiligheidsincidenten. We doen dit door:

- **incidentbehandeling** te **coördineren** en erover te **adviseren**
- **bedreigingen te evalueren**
- **alarmen en waarschuwingen te publiceren** op www.cert.be, Twitter en via RSS
- **adviezen en rapporten te publiceren**
- **incidentbehandelingen** te ondersteunen of te coördineren.

CERT.be – een netwerk van experts tot uw dienst

1 • Proactief

Mogelijk weet u zelf niets van een aanval en weten wij het voor u het merkt. Als het om een ernstig incident gaat nemen we zelf met u contact op.

2 • Op uw initiatief

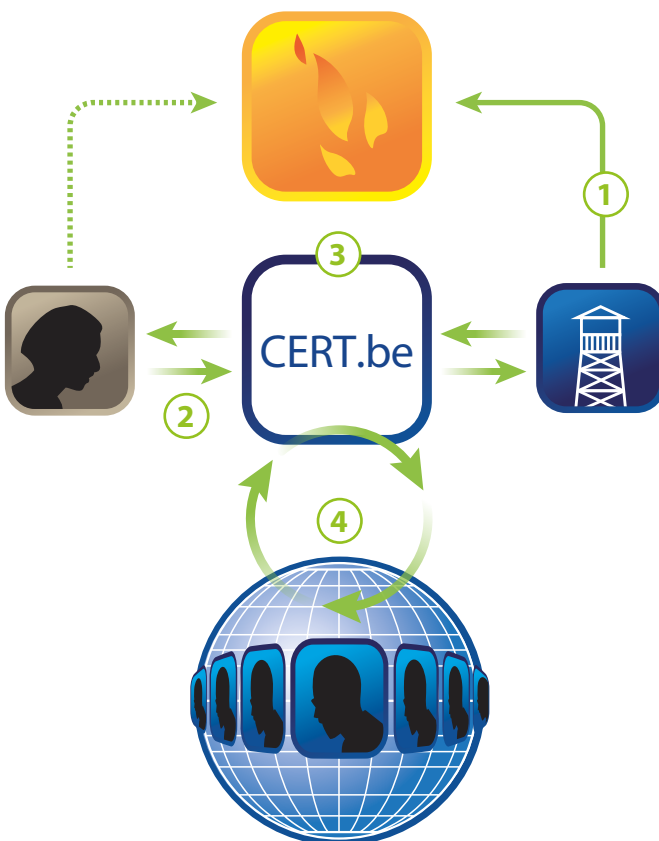
U bent het slachtoffer van een cyberincident of u denkt dat te zijn. U neemt zelf contact op met CERT.be

3 • Interne consultatie

Onze expert schat op basis van uw aangifte de ernst van de situatie in. Hij consulteert zijn interne contacten. We koppelen naar u terug.

4 • Andere experts

In geval van een ernstig incident spreken wij onze andere kanalen aan. Door intense samenwerking en uitwisseling van informatie met ons netwerk van externe experts, o.a. van andere CERTs, proberen we uw probleem zo snel mogelijk van de baan te hebben.



Beveiligingsbeheer

Onze managementdiensten zijn gericht op de ontwikkeling van een kwaliteitsvol beveiligingsbeheer. Wij stellen onze expertise ter beschikking aan bedrijven en organisaties die eigen CERT-activiteiten willen opzetten. Een bedrijfsintern cyber emergency team vergemakkelijkt de communicatie tussen CERT.be en uw organisatie enerzijds en tussen uw organisatie en cyber emergency teams in andere organisaties anderzijds.

Omdat incidenten dikwijls uw bedrijf overschrijden is een dergelijke communicatie heel nuttig. Cyber emergency teams kunnen onderling in alle discretie tips en ervaringen uitwisselen om zo incidenten efficiënt te beheren en te behandelen.

Internationale samenwerking

Omdat netwerkbedreigingen vaak vanuit het buitenland komen, werkt CERT.be binnen een wereldwijd netwerk van cyberbeveiligingsexperts. Wanneer uw bedrijf een elektronische aanval, hack of inbraakpoging opmerkt en ons dat meldt, dan nemen wij contact op met onze buitenlandse collega's om de oorsprong van de problemen op te sporen. De internationale samenwerking verloopt via cyberbeveiligingsexperten die elkaar persoonlijk kennen en de informatie-uitwisseling gebeurt in alle discretie, zonder gegevens over betrokken bedrijven te vermelden.

“

Omdat netwerkbedreigingen vaak vanuit het buitenland komen, werkt CERT.be binnen een wereldwijd netwerk van cyberbeveiligingsexperts.

”



Traffic Light Protocol (TLP)

Net als andere cyber emergency teams, maakt CERT.be gebruik van een Traffic Light Protocol (TLP) om het uitwisselen van informatie op een veilige manier te laten verlopen en aan te moedigen.

- **Rood** – Info uitsluitend bestemd voor de rechtstreeks geadresseerden
- **Oranje** – Info voor een organisatie, eventueel beperkt tot bepaalde personen van de organisatie
- **Groen** – Info voor een gemeenschap, niet te verspreiden op het internet.
- **Wit** – Info die vrij verspreid mag worden, voor zover de verspreiding niet strijdig is met de wet (bijvoorbeeld de wet op het auteursrecht).



Wat kan uw bedrijf zelf doen?

- ✓ **Wees proactief.** Breng uw kwetsbaarheden in kaart (vulnerability management) en bepaal hoe u ze gaat aanpakken door systemen en software te verbeteren en up-to-date te houden (patch management).
- ✓ **Gebruik beveiligde software** en appliances zoals firewalls.
- ✓ Verwacht niet alles van één technologie. **Combineer oplossingen.**
- ✓ Vergeet de **menselijke factor** niet. Bewustmakingsprogramma's zijn heel belangrijk om de aandacht van werknemers op de veiligheidsproblematiek te vestigen. Combineer deze bewustmaking met een charter waarin u vastlegt wat werknemers wel en niet mogen.
- ✓ **Overdrijf niet met verbieden.** Een te strikt veiligheidsbeleid kan mensen aanzetten de regels te omzeilen met eigen devices zoals smartphones en tablets.
- ✓ Overweeg om **eigen CERT-activiteiten op te starten**, met een verantwoordelijke voor IT-security. Een intern erkend persoon die de veiligheidsproblematiek kent en waarmee andere veiligheidsspecialisten in vertrouwen kunnen spreken, is erg belangrijk.
- ✓ Stel een **wachtwoordbeleid** op en geef uw medewerkers tips om veilige en verschillende wachtwoorden te gebruiken.
- ✓ **Wees voorbereid:** u kunt altijd slachtoffer worden. Zorg dat u weet hoe u met een incident moet omgaan. Hou geteste back-ups en uw log- en monitoringsystemen paraat om problemen snel te detecteren en aan te pakken.

Bedrijven **getuigen**

Cybercriminaliteit is niet nieuw, maar het neemt tegenwoordig andere, vaak heel **georganiseerde vormen** aan. Organisaties en bedrijven die er het slachtoffer van waren, doen er alles aan om het niet opnieuw te hoeven meemaken. **Dankzij hun openheid** kan CERT.be ernstige incidenten **helpen voorkomen of oplossen**. De organisaties op de volgende pagina's vonden de weg naar CERT.be.

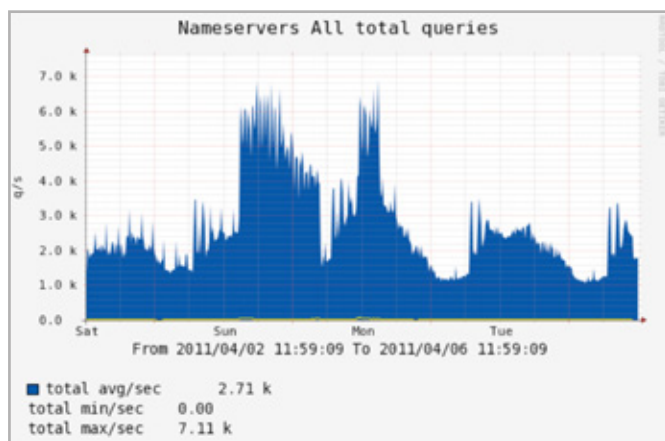


“Open communicatie en het delen van informatie zijn belangrijk”

Philip Du Bois
General Manager DNS.be



“Begin april 2011 kregen onze nameservers ineens zes keer meer aanvragen (queries) te verwerken dan normaal. Achter die verhoogde activiteit zat een netwerk van gehackte computers, dat mailservers van .be- domeinnamen probeerde te misbruiken. Dat gebeurde tevergeefs, want wij slaan geen mailservergegevens op over onze domeinnamen.



Wij merkten het verdachte verkeer op omdat we de aard van queries, het bandbreedtegebruik en de status van onze nameservers via een monitoringsysteem controleren. We hebben CERT.be verwittigd, en zij hebben een analyse

gemaakt op basis van de data die we van het incident verzamelden. Die open communicatie en het delen van informatie zijn heel belangrijk. Het versterkt ook je eigen expertise.

Uiteindelijk kan iedereen het slachtoffer worden van een cyberaanval, ook als je enorm goed beveiligd bent. Daarom raad ik aan om proactief te zijn: leg vooraf al contact met de specialisten van CERT.be. Hun nummer is als dat van de brandweer of het ziekenhuis. Dat moet gewoon klaar liggen bij je IT-team.”

DNS.be beheert 1,25 miljoen .be-domeinnamen. Onlangs heeft DNS.be van de Vlaamse overheid en van de Brusselse overheid de toestemming gekregen om ook de nieuwe extensies .vlaanderen en .brussels te beheren.

“

Beveiliging van de computerinfrastructuur is geen luxe ”

Simon François

Netwerk- en beveiligingsverantwoordelijke ULg



“In 2010 kreeg de ULg een DoS-aanval (Denial of Service) te verduren, gericht tegen de servers van het departement biotechnologie. De aanval bestond uit het **massaal versturen van miljoenen vervalste DNS-pakketten** met een bandbreedte van 1,5 Gbit/s. Onze twee perimeter firewalls werden geneutraliseerd en de internettoegang van de universiteit was volledig geblokkeerd.

Onze veiligheidsexperten konden het probleem vlug identificeren en we hebben onmiddellijk de hulp van CERT.be ingeroepen. Na een snelle analyse van de aanval heeft CERT.be ingegrepen via de servers van Belnet, het nationale onderzoeksnetwerk waarop ook de ULg is aangesloten. Het **kwaadaardige netwerkverkeer werd zo afgeleid** zodat het ons netwerk niet meer kon bereiken.

Het mag duidelijk zijn dat cyberaanvallen zeer vaak gebeuren, en niet enkel bij anderen. We hebben kunnen vaststellen dat CERT.be klaarstaat om iedereen een efficiënte oplossing te bieden.”

De ULg (Université de Liège) werd gesticht in 1817. Ze telt 5000 personeelsleden, waaronder 3300 met een onderwijs- en onderzoeksopdracht. Eén van de prioriteiten van de ULg is internationale samenwerking. Daarom onderhoudt de ULg contacten met meer dan 600 instellingen wereldwijd.

www.ulg.ac.be

“ CERT.be: de link naar buitenlandse expertise”

Paul Boons,
Agfa Information Security Officer



“We voeren bij Agfa een proactief veiligheidsbeleid. Informatie-uitwisseling is daarin cruciaal. Voor ons is het belangrijk dat dat op een internationale schaal gebeurt. Ten eerste omdat Agfa internationaal actief is en dat geldt dus ook voor ons datanetwerk. Ten tweede omdat cybercriminaliteit een **typisch grensoverschrijdend fenomeen** is. Zo zijn we bijna vanzelf bij CERT.be uitgekomen.

CERT.be maakt deel uit van een internationaal professioneel netwerk. Dat is nuttig in het geval van een echte cyberbedreiging, maar het biedt ook preventief een belangrijke meerwaarde. Ze zijn vaak heel snel op de hoogte van concrete bedreigingen en kunnen ons via de contacten met hun internationale collega's **relevante informatie aanreiken ter voorkoming of bestrijding** van een cyberbedreiging.

CERT.be organiseert ook regelmatig **seminaries over cybercriminaliteit**. We sturen onze mensen graag naar dergelijke internationale ontmoetingsplaatsen. Het is de ideale manier om up-to-date te blijven en info uit te wisselen met collega's van andere bedrijven.

Ik zie voor CERT.be een belangrijke rol weggelegd voor wat betreft de uitwisseling van technische informatie met bedrijven. Als we bepaalde technische patronen herkennen, kunnen we bij CERT.be nagaan of dit ook voor andere bedrijven gekende technische patronen zijn. Het **uitwisselen van die technische specificaties**, al dan niet anoniem via CERT.be, kan helpen om bedrijfsnetwerken op een efficiënte manier af te schermen.”

Agfa is wereldleider op het vlak van beeldvorming. Het bedrijf ontwikkelt, produceert en verdeelt analoge en digitale producten en systemen om beelden te maken, te verwerken en te reproduceren. Ze zijn vooral gekend voor hun oplossingen voor de grafische en de medische sector. De hoofdzetel van Agfa is gevestigd in Mortsel bij Antwerpen. Het bedrijf produceert ook in de VS, Duitsland en China en heeft in meer dan 40 landen verkoopskantoren. De afdeling Agfa ICS (Information & Communication Services) stelt wereldwijd 460 mensen te werk en beheert en beveiligd de netwerkverbindingen tussen 100 locaties. Agfa ICS is ook verantwoordelijk voor de datacenters van Agfa in o.a. België, Duitsland en Canada.

Praktische informatie



Centraal meldpunt

CERT.be is het centraal meldpunt voor cyberveiligheidsproblemen. U kunt bij ons kosteloos terecht met uw vragen over beveiliging en risicobeheer.

Algemene vragen

Via e-mail naar info@cert.be.

Per telefoon op 02 790 33 33, op werkdagen van 9 tot 17 uur

Veiligheidsincidenten melden

Via e-mail naar cert@cert.be. Confidentiële informatie kunt u versleutelen met onze publieke sleutel.

Meer gegevens hierover vindt u op www.cert.be

Per telefoon op 02 790 33 85

Bij de melding van een cyberincident

Geef altijd uw volledige contactgegevens en een zo volledig mogelijk antwoord op de volgende vragen:

- ✓ Wanneer is het incident begonnen?
- ✓ Wie hebt u al op de hoogte gebracht?
- ✓ Om welk type incident gaat het: DDoS, malware, ...?
- ✓ Is het incident nog bezig? Wat is het verloop?
- ✓ Wat is de impact van het incident?
- ✓ Hebt u reeds maatregelen genomen?
- ✓ Beschikt u over logs of andere nuttige data?
- ✓ Wat verwacht u van uw melding?
- ✓ Wenst u een aangifte te doen bij de politie?



Welke partijen zijn betrokken bij CERT.be?

CERT.be is het federale cyber emergency team, opgericht in 2009, dat wordt uitgebaat door Belnet, het Belgisch nationaal onderzoeksnetwerk, in opdracht van Fedict.

Belnet beheert het onderzoeksnetwerk voor de Belgische universiteiten, hogescholen, onderzoekscentra en overheidsdiensten.

Belnet richtte al snel een eigen CERT op om zijn eigen netwerk te bewaken en zijn eigen klanten te informeren. Vóór de oprichting van CERT.be was het Belnet CERT de facto het internationale aanspreekpunt voor alles wat met de Belgisch nationale netwerkbeveiliging te maken had.

Fedict (Federale Overheidsdienst voor Informatie- en Communicatietechnologie) werkt aan e-government en helpt federale overheidsdiensten hun service aan burgers, ondernemingen en ambtenaren te verbeteren met behulp van ICT.

Fedict ligt aan de basis van tal van innoverende technologieprojecten, zoals Tax-on-web, het meldpunt eCops en de elektronische identiteitskaart.

Meld uw cyberincidenten in alle discretie

U bent misschien niet de enige onder aanval...

Anderen hebben misschien al een oplossing gevonden...

Uw oplossing kan anderen helpen...



cert@cert.be



02 790 33 85



CERT.be
The Federal Cyber Emergency Team

Belnet – CERT.be
Louizalaan 231
1050 Brussel

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