12 GOUDEN REGELS INZAKE ICT-SECURITY

CIBG-KATERN 36

PRAKTISCHE GIDS


CRIME SCENE-DO NOT ENT

12 GOUDEN REGELS INZAKE ICT-SECURITY

Als overheidsadministratie moet u beseffen dat computercriminelen ook bij u kunnen toeslaan. Of het nu criminelen zijn die gegevens wensen te vernietigen of geld willen afpersen, de mogelijke gevolgen van ernstige inbreuken op uw ICT-security zijn per definitie zeer ernstig te nemen.

De public sector dient "best in class" te zijn wanneer het op computerbeveiliging aankomt. Wij liggen immers nog meer onder de loep van de pers en de publieke opinie wanneer het fout loopt. En dat is normaal. We behandelen immers vaak de privé-gegevens van heel wat burgers.

Een overheidsorganisatie als de uwe dient met andere woorden haar informatiesystemen voldoende te beschermen dankzij een professioneel veiligheidsplan. Wij steken u daar graag een handje bij toe.

Het Centrum voor Informatica voor het Brusselse Gewest helpt u al meer dan 25 jaar bij het uittekenen van uw ICT-beleid. Vandaag zetten we graag een stapje verder en wensen we u ook te begeleiden bij het opzetten van een professioneel ICT-securityplan.

Met deze kleine praktische gids reiken we u alvast een aantal goede praktijken aan, die nauwelijks geld kosten, makkelijk toepasbaar zijn en die een groot deel van de risico's wegnemen.

Hervé FEUILLIEN
Directeur-generaal

Robert HERZEELE
Adjunct Directeur-generaal


CONNECT
click
ON
credit
PAY
PAY CREDIT CARD
CLOUD
Protection!
DATA
DATA
Lock!
LOG IN :
USERNAME
PASSWORD

INHOUDSOPGAVE

WAAROM EEN ICT-SECURITY PLAN?

Pc's, laptops, tablets, smartphones zijn deel geworden van ons leven, zowel privé als professioneel. Vaak worden de beveiligingsregels bij het gebruik van deze toestellen nogal eens uit het oog verloren. Nieuwe technologieën houden immers ook nieuwe risico's in.

Gevoelige gegevens (privé-gegevens van burgers, contracten, lopende projecten, etc.) kunnen door hackers gestolen worden of in verkeerde handen terechtkomen bij verlies of diefstal van uw pc, smartphone, tablet of laptop. Dergelijke voorvallen leiden tot economische en financiële verliezen en imagoschade voor uw gehele organisatie.

Die gevaren kunnen we echter vrij goed beheersen aan de hand van een reeks "best practices" die nauwelijks of zelfs geen geld kosten en makkelijk ook binnen uw organisatie onmiddellijk toepasbaar zijn.

Deel ze met uw medewerkers, zet ze op uw intranet, zodat ook zij bewust worden van het belang van ICT-security.

1. MIJN WACHTWOORD VERDIENT MIJN AANDACHT

Een wachtwoord is een authenticatiemiddel dat met name gebruikt wordt om toegang te krijgen tot computerapparatuur of tot gegevens. Om uw gegevens voldoende te beschermen, moet u wachtwoorden kiezen die moeilijk op te sporen zijn met geautomatiseerde tools, of moeilijk te raden door derden.

EEN AANTAL GOUDEN REGELS

- Gebruik geen korte wachtwoorden. Een achttal tekens is toch het minimum. Meer is nog beter.
- Geef de voorkeur aan wachtwoorden die bestaan uit combinaties van hoofdletters, kleine letters, cijfers, speciale tekens.
- Vermijd persoonlijke wachtwoorden zoals een naam, geboortedatum, naam van uw huisdier, enz. Deze zijn vaak gemakkelijker te vinden dan u denkt.
- Gebruik bij voorkeur woorden die niet in het woordenboek staan, dus die niet gemakkelijk uit te vissen zijn door automatische zoekmachines.
- Zorg ervoor dat u regelmatig uw wachtwoorden verandert.
- Bewaar uw wachtwoorden nooit in een onbeveiligd bestand of op een stukje papier.
- Laat uw wachtwoorden niet onthouden in een browser als u surft op een openbare of gedeelde computer zoals bijvoorbeeld in een internetcafé.
- Leg binnen uw organisatie alles vast in richtlijnen en communiceer deze regels duidelijk. Zorg ook dat ze worden nageleefd.

2. UW SOFTWARE DIENT REGELMATIG GEÜPDATET

Elk besturingssysteem (Android, iOS, MacOS, Linux, Windows,...) en elke software of toepassing heeft zwakke punten die door hackers kunnen worden misbruikt. Softwaremakers brengen gewoonlijk regelmatig veiligheidsupdates uit om die zwakke punten weg te werken. Toch zijn er nog steeds heel wat gebruikers die deze updates niet installeren.

EEN AANTAL GOUDEN REGELS

- Zorg ervoor dat alle veiligheidsupdates automatisch geïnstalleerd worden telkens wanneer dat mogelijk is. Anders moet u de beschikbare veiligheidspatches zelf manueel downloaden en installeren en dat wordt vaak vergeten.
- Werk uitsluitend met de officiële websites van de softwaremakers.
- Werk uitsluitend met recente besturingssystemen waarvoor nog updates ter beschikking worden gesteld.
- Laat binnen uw organisatie een volwaardig updatebeleid uittekenen en laat dit beleid daadwerkelijk en stipt toepassen.

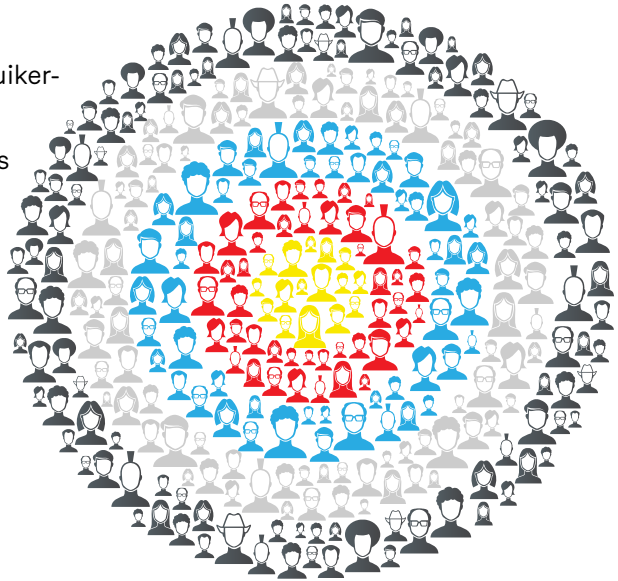
3. WIE ZIJN MIJN GEBRUIKERS?

Wanneer u op uw pc inlogt, hebt u bepaalde gebruiksrechten op dat apparaat. Doorgaans onderscheiden we rechten als «gebruiker» en rechten als «administrator».

- Voor het dagelijkse gebruik van uw pc (surfen, mails lezen, werken met kantoorsoftware,...) volstaat een gebruiker-account.
- De administrator-account dient om de algemene werking van de pc aan te passen (gebruiker-accounts beheren, beveiligingsbeleid wijzigen, software installeren of updaten,...). Via de administrator-account is het mogelijk om verregaande ingrepen op uw pc door te voeren.

EEN AANTAL GOUDEN REGELS

- Zorg dat alle medewerkers enkel hun eigen gewone gebruiker-account raadplegen.
- Zorg dat enkel uw IT-medewerkers administrator-accounts kunnen gebruiken.
- Zorg voor een "**in-procedure**" om aan nieuwe medewerkers de toegangsrechten tot de computersystemen correct en stipt toe te kennen.
- Ook een **"out-procedure"** is belangrijk zodat de toegangsrechten van medewerkers opnieuw worden ingetrokken als deze uw organisatie verlaten.



4. MAAK REGELMATIG EEN BACK-UP

Om uw gegevens te beveiligen is het zeer aangeraden om regelmatig (dagelijks of wekelijks) een back-up uit te voeren. Zo kunt u uw gegevens terugzetten in geval van een defect of wanneer u het slachtoffer bent van een cyberaanval.

Voor het back-uppen van uw gegevens kunt u gebruikmaken van externe dragers, zoals een externe harde schijf, een USB-stick of ook een beschrijfbare cd of dvd. Bewaar deze nooit naast uw pc en ook op een veilige manier. Zo kunt u voorkomen dat uw back-up vernietigd wordt bij brand of verdwijnt bij diefstal.

EEN AANTAL EXTRA TIPS

- Gebruik geen « cloud »-diensten om vertrouwelijke gegevens te bewaren tenzij de vertrouwelijkheid gegarandeerd wordt zoals bij het Centrum voor Informatica voor het Brusselse Gewest.
- Bescherm de vertrouwelijkheid van uw gegevens door ze te versleutelen en zo onleesbaar te maken voor onbevoegden.

5. VEILIGE WIFI

Wifi is praktisch. Vergeet echter niet dat indringers slecht beveiligde draadloze netwerken kunnen misbruiken en zo gemakkelijk uw privé gegevens kunnen onderscheppen.

EEN AANTAL GOUDEN REGELS

- Zorg ervoor dat uw pc beschermd is door een antimalware-programma.
- Maak enkel gebruik van bekende openbare wifi-netwerken of hotspots. Hotels, luchthavens, en dergelijke leveren meestal veilige toegangen maar enig gezond wantrouwen is nooit overbodig. Ook Urbizone in het Brussels Hoofdstedelijk Gewest is een beveiligde toegang.
- Blijf bewust van de risico's om persoonlijke of vertrouwelijke gegevens (in het bijzonder vertrouwelijke e-mails, financiële verrichtingen etc.) te versturen via een wifiverbinding
- Laat geen klanten, leveranciers of andere derden toe op uw corporate wifinetwerk als dit verbonden is met uw intern netwerk.

6. SMARTPHONE OF TABLET, WEES VOORZICHTIG!

Uw persoonlijk mobieltje professioneel gebruiken is modern en gemakkelijk maar u zorgt er toch best voor dat uw professionele gegevens zo veilig mogelijk zijn. Die kleine toestellen worden makkelijk uit het oog verloren en even niet opletten en u bent al snel het slachtoffer van gauwdieven.

EEN AANTAL GOUDEN REGELS

- Vermijd om uw pincode op te slaan in de configuratie van uw mobieltje.
- Gebruik naast uw pincode ook een wachtwoord om de toegang tot uw apparaat te beveiligen. Stel uw toestel zo in dat het automatisch blokkeert na een aantal seconden wanneer u het niet gebruikt.
- Zorg ervoor dat uw mobieltje indien mogelijk beschermd is door een antimalware-programma.
- Installeer bewust enkel de apps die u nodig hebt en ga na tot welke gegevens zij toegang kunnen hebben voordat u ze downloadt (geografische informatie, contacten, telefoonoproepen, ...). Sommige apps vragen toegang tot gegevens die ze voor hun werking eigenlijk niet nodig hebben. Ze kunnen ook spyware bevatten.
- Maak regelmatig een back-up op een externe drager. Die gegevens kunt u nodig hebben om uw apparaat in zijn oorspronkelijk toestand te herstellen.

7. TIPS VOOR VEILIG REIZEN

Dankzij laptops, smartphones en tablets zijn dienstreizen en de uitwisseling van data een stuk makkelijker geworden. Dergelijke toestellen meenemen houdt echter risico's in voor de gevoelige informatie die zij bevatten, bijvoorbeeld bij verlies of diefstal.

EEN AANTAL GOUDEN REGELS

...voor u vertrekt

- Neem enkel die toestellen mee (laptop, smartphone, tablet) die u nodig hebt.
- Zorg ervoor dat uw toestellen enkel de strikt nodige informatie bevatten.
- Zorg voor een degelijke anti-malware.
- Maak een back-up van uw gegevens. Bij verlies zult u die nodig hebben.
- Zorg voor een moeilijk te vinden wachtwoord dat niet automatisch onthouden wordt. (zie tip 1).

...tijdens de reis

- Verlies uw toestel nooit uit het oog.
- Schakel wifi en Bluetooth enkel aan als u die nodig hebt.
- Verwittig uw organisatie onmiddellijk bij verlies of diefstal.
- Laat onmiddellijk uw simkaart blokkeren bij verlies of diefstal.
- Verwittig onmiddellijk uw organisatie wanneer uw toestel door buitenlandse autoriteiten is gecontroleerd of in beslag werd genomen.

- Sluit uw toestel niet aan op systemen die u niet vertrouwt.
- Gebruik uw eigen USB-stick of memory card als u gegevens moet uitwisselen of gebruiken op een ander toestel. Wis de gegevens vervolgens met een veilig wisprogramma.
- Laat niet toe dat derden hun toestellen op die van u aansluiten (smartphone, USB-stick, etc.).

...na de reis

- Wijzig de wachtwoorden die u tijdens uw reis gebruikt hebt.
- Laat bij twijfel uw toestel na een dienstreis nakijken.
- Maak nooit gebruik van USB-sticks die u zou hebben gevonden of zelfs gekregen van onbekenden (op een beurs, tijdens een vergadering, etc.).

8. VEILIG MAILEN

Mails en de bijbehorende bijlagen spelen doorgaans een centrale rol bij computeraanvallen (frauduleuze mails, bijlagen met virus, ...).

EEN AANTAL GOUDEN REGELS

- Zorg ervoor dat uw mailprogramma ook automatisch beschermd wordt door een anti-malware.
- De identiteit van een afzender is nooit gewaarborgd: controleer of de inhoud van een bericht een duidelijk verband heeft met de veronderstelde afzender. Neem bij twijfel rechtstreeks telefonisch contact op met de afzender van de mail.
- Bekijk alle bijlagen in een mail kritisch en open geen verdachte bijlagen zeker als die afkomstig zijn van onbekende afzenders. Schakel zeker het automatisch openen van dergelijke bestanden uit!
- Indien er in een mail links zitten, ga dan na of het adres achter deze link wel overeenkomt met de link zelf. Meestal kan dat door met de muis even boven de link te gaan staan zonder deze aan te klikken. Op die manier kunt u de juistheid ervan controleren. Klik dus niet zomaar op elke link die u wordt toegestuurd. Dit is dé klassieke manier om een virus binnen te halen.
- Beantwoord nooit een mail die u vertrouwelijke of persoonlijke informatie vraagt (bijv. geheime code en/of nummer van uw bankkaart). Bonafide bedrijven zoals banken en providers doen dit nooit! Het betreft hier «phishing»-aanvallen, die er enkel op uit zijn om u gegevens te ontfutselen. Wis deze mails onmiddellijk!

9. DOWLOADEN ZONDER ZORGEN

Wanneer u downloadt van dubieuze websites, dan loopt u een groot risico illegale of geïnfecteerde programma's op uw pc te installeren die virussen of Trojaanse paarden bevatten. Op die manier kunnen mensen met kwade bedoelingen van op afstand de controle over uw pc overnemen, uw persoonlijke gegevens stelen, etc.

EEN AANTAL GOUDEN REGELS

- Download enkel van officiële of van betrouwbare websites.
- Zorg ervoor alle voorstellen om aanvullende software te installeren, af te vinken of uit te schakelen.
- Schakel het automatisch openen van gedownloade bestanden uit.
- Zorg dat gedownloade bestanden steeds automatisch gecontroleerd worden op malware vooraleer die te openen.

10. WEES WAAKZAAM BIJ ONLINE AANKOPEN

Wanneer u online aankopen verricht, bestaat het gevaar dat uw bankgegevens door aanvallers worden onderschept. Vooraleer u online een betaling uitvoert voor een aankoop moet u de e-commercesite op een aantal punten aftoetsen.

EEN AANTAL GOUDEN REGELS

- Kijk of de aanduiding « https:// » bij het begin van het internetadres aanwezig is; dit wijst op een beveiligde web-omgeving.
- Controleer of het adres van de website correct gespeld is en dat er bijvoorbeeld geen tikfouten in staan.
- Geef de voorkeur aan een betaalmethode via een officiële betaalinstelling. Banken en betaalinstellingen gebruiken doorgaans een bankkaartlezer waarmee een code gegenereerd moet worden.
- Geef nooit de pincode van uw bankkaart door.

11. HOU PERSOONLIJK EN PROFESSIONEEL GEBRUIK STRIKT GESCHEIDEN

U moet geen minister zijn om te beseffen dat u privé- en professioneel gebruik van uw laptop, smartphone, e-mail best strikt gescheiden houdt. Het professioneel gebruik van privé toestellen op kantoor (dit heet “Bring your own device”) kan uw werk makkelijker maken en vele bedrijven laten dat ook toe. U houdt er vast aan dat uw privé-gegevens vertrouwelijk blijven. Uw organisatie heeft net dezelfde wensen wanneer het gaat om haar vertrouwelijke bedrijfsgegevens. De oorzaken van een data-lek zijn meestal van menselijke aard, met opzet of door een vergissing.

EEN AANTAL GOUDEN REGELS

- Houd persoonlijk gebruik en professioneel gebruik bij voorkeur strikt gescheiden.
- Schakel professionele mail niet automatisch door naar een persoonlijk mailadres.
- Bewaar geen professionele gegevens op persoonlijke mobiele apparaten of op persoonlijke online opslagsystemen.
- Gebruik geen privé mobiele dragers (USB-stick, externe harde schijf, enz.) binnen uw organisatie.

12. BEWAAK UW DIGITALE IDENTITEIT

Besef dat u tijdens het surfen op het Internet heel wat sporen achterlaat. Mensen met kwade bedoelingen zijn steeds op zoek naar persoonlijke informatie uit winstbejag of om uw identiteit te stelen. Zij proberen uw wachtwoorden te vinden om toegang te krijgen tot uw gegevens om die te kunnen misbruiken.

EEN AANTAL GOUDEN REGELS

- Geef op een website of in een formulier enkel gegevens door die noodzakelijk zijn. Noodzakelijk in te vullen gegevens worden vaak duidelijk aangeduid.
- Vermijd op een website toestemming te geven om uw gegevens te bewaren of te delen.
- Plaats zo weinig mogelijk privé of professionele informatie op sociale netwerken. Sociale netwerken zoals Facebook durven nogal eens een loopje te nemen met de nationale wetgeving die u probeert te beschermen.
- Geef zo weinig mogelijk privé of professionele informatie door tijdens chatsessies.
- Controleer regelmatig uw beveiligings- en vertrouwelijkheidsparameters op sociale netwerken.
- Gebruik zo weinig mogelijk uw officiële privé en professionele e-mailadressen behalve op websites waarvan u weet dat die te vertrouwen zijn. Gebruik bij twijfel een pseudo of alternatief e-mailadres dan zult u ongetwijfeld veel spam vermijden.

13. MIJN EIGEN TIPS

Het Centrum voor Informatica voor het Brusselse Gewest heeft als taak het gebruik van informatie- en communicatietechnieken te organiseren, te promoten en te verspreiden zowel bij plaatselijke overheden als bij de verschillende besturen van het Brussels Hoofdstedelijk Gewest.

Het CIBG heeft binnen deze context als opdracht te informeren, met name door de publicatie van Katernen die een beeld vormen van zijn activiteiten, projecten of de evolutie van de technologieën.

RECENTE PUBLICATIES

2013

2014

2015

De Katernen van het CIBG zijn beschikbaar in elektronisch formaat en te vinden op cibg.brussels
Voor meer informatie stuurt u een mailtje naar communicatie@cibg.brussels.

cibg.brussels
IT is for you

Redactie en coördinatie: Dienst Communicatie CIBG
Gedrukt met plantaardige inkt op papier afkomstig uit duurzaam beheerde bossen (FSC-label).

Verantwoordelijke uitgever: Hervé Feuillien
CIBG Kunstlaan 21 - 1000 Brussel
T 32 2 282 47 70 F 32 2 230 31 07
cibg.brussels - communicatie@cibg.brussels
@CIRB_CIBG