

The background of the slide is a dark blue grid pattern. Overlaid on this grid are several circular icons in a lighter blue color. These icons include a Wi-Fi symbol, an envelope, a document with a checkmark, a gear with a wrench and screwdriver, a camera, a Facebook 'f' logo, a Twitter bird, and a plus sign with a link icon. A large, realistic hand is shown from the side, holding a blue padlock. The padlock is positioned over the grid and icons, with its shackle pointing upwards.

Hacking bij Stad Diest

Myriam Parys

LockBit Black

**All your important files are stolen and encrypted!
You must find c3pWHbBNT.README.txt file
and follow the instruction!**

Onbekenden hebben onze computers gehackt. Daardoor ligt de dienstverlening plat.

We stellen alles in het werk om onze systemen zo snel mogelijk terug operationeel te krijgen. Maar onze loketdiensten werken niet, inwoners een afspraak geven, lukt dus niet en we kunnen ook geen e-mails ontvangen of beantwoorden.

Onze website blijft beschikbaar en ook voor dringende zaken blijven we telefonisch bereikbaar.

An illustration of a person's legs and hands holding a light blue rectangular sign. The person is standing on a red background. The sign has the text 'Sorry, voor het ongemak' written on it in bold black letters.

**Sorry,
voor het
ongemak**

PLAY NEWS

CONTACT

FAQ

We have a small queue when loading full dumps, wait, all published will certainly be loaded.

Hilldrup

Stafford, Virginia, USA

www.hilldrup.com

views: 227

added: 2022-12-09

publication date: 2022-12-17

8 DAYS BEFORE PUBLICATION

???????

Resistencia, Chaco Province, Argentina

www.????????.com.ar

views: 145

added: 2022-12-09

publication date: 2022-12-17

8 DAYS BEFORE PUBLICATION

????

Lake Washington Blvd, Washington, USA

www.?????.com

views: 282

added: 2022-12-08

publication date: 2022-12-16

7 DAYS BEFORE PUBLICATION

????????? ???? ?????

Hastings St, Vancouver, Canada

www.????.????

views: 339

added: 2022-12-06

publication date: 2022-12-13

4 DAYS BEFORE PUBLICATION

UJV Rez

Husinec, Praha, Czech Republic

www.ujv.cz

views: 323

added: 2022-12-06

publication date: 2022-12-14

5 DAYS BEFORE PUBLICATION

Wrota Mazowsza

Poland

www.wrotamazowsza.pl

views: 385

added: 2022-12-06

publication date: 2022-12-14

5 DAYS BEFORE PUBLICATION

Conseil departemental - Alpes-Maritimes

Nice, France

www.departement06.fr

views: 1481

added: 2022-11-18

publication date: 2022-11-28

PUBLISHED

Origin Property Company Limited

Samut Prakan, Thailand

www.origin.co.th

views: 1754

added: 2022-11-18

publication date: 2022-11-27

PUBLISHED FULL

Itsgroup

Boulogne-Billancourt, France

www.itsgroup.com

views: 1980

added: 2022-11-10

publication date: 2022-11-17

PUBLISHED FULL

Ministry of Transport and Public Works

Montevideo, Uruguay

www.mtop.gub.uy

views: 1458

added: 2022-11-09

publication date: 2022-11-18

PUBLISHED

Leadtek

New Taipei City, Taiwan

www.leadtek.com

views: 1565

added: 2022-11-07

publication date: 2022-11-16

PUBLISHED

PVFCCo

Ho Chi Minh, Vietnam

www.dpm.vn

views: 1506

added: 2022-11-03

publication date: 2022-11-17

PUBLISHED

Worst case scenario

- geen e-mail @gemeente.be
- geen laptops
- geen desktops
- geen wifi
- geen bekabeld netwerk
- geen interne telefooncentrale
- geen netwerkprinters
- geen netwerkschijven met data
- geen toepassingen die op de lokale server draaien
- geen prikklok
- geen gebruik van usb sticks

Impact op dienstverlening

- geen boekhouding (geen betalingen)
- geen registratie geboorte/overlijden
- geen loonadministratie (salarissen)
- geen administratie sociale dienst (leefloon)
- geen omgevingsvergunningen
- geen digitale registratie kinderen in kinderopvang
- geen digitale registratie ontlenden boeken in bib
- geen telefonische bereikbaarheid van een aantal vestigingen
- geen werkopdrachten arbeiders
- geen ticketingsysteem cultureel centrum
- geen registratie post
- geen kassasysteem zwembad
- geen werkend afsprakensysteem
-



Beste collega's, ik moet helaas meedelen dat stad Diest gehackt is. Jullie zullen zelf ook al wel gemerkt hebben dat alles plat ligt. Recentelijk werden verschillende andere lokale besturen gehackt, onlangs nog Antwerpen, en nu schijnt Diest aan de beurt te zijn. Wij zitten momenteel samen in crisioverleg op het stadhuis. Er is momenteel nog veel onduidelijk: wie hier achter zit, hoe lang dit zal duren en wat de totale impact is. Ik tracht jullie de komende uren of dagen te informeren wanneer er meer nieuws is.

11:41 ✓

Ik zou jullie het volgende willen vragen: 1) gezien wij niet kunnen mailen is de communicatie naar al ons personeel zeer moeilijk. Ik wil jullie vragen om zelf de personeelsleden van jullie dienst te verwittigen. 2) Gezien het stadsnetwerk en alle applicaties niet beschikbaar zijn, is thuiswerk geen optie. Ik wou willen vragen om personeelsleden zoveel mogelijk zinvolle taken te geven: bvb klassament, opruimen dossiers, lezen en voorbereiden dossiers, ... 3) Omdat prikklok niet werk, graag uren manueel bijhouden. Wij hopen dat deze situatie niet te lang duurt, maar hebben hier voorlopig geen zicht op.



To do

- Lokale crisiscel samenroepen. Computer crime unit, CERT, DPO en externe ICT-experten inschakelen.
- In lockdown gaan (afsluiten van de netwerkconnecties om de schade te beperken).
- Communicatie zo breed mogelijk (burgers, personeel, leveranciers ...).
- Via business impact analyse bepalen welke applicaties zo snel mogelijk terug beschikbaar moesten komen en prioriteiten stellen.
(Burgerzaken! Boekhouding! Uitbetaling lonen! Uitbetaling leeflonen! e.d.)
- Kijken welke back ups beschikbaar zijn (intern en bij externe leveranciers).
- Opties tot datarecuperatie maximaal bekijken.
- Nieuwe veilige IT-omgeving opbouwen. In veilige IT-omgeving noodloketten bouwen.

Stap 1: Bepaal de RTO (Recovery Time Objective)

Proces	Meer dan 2 uur	Meer dan 2 dagen	Meer dan 2 weken	Meer dan 2 maanden	Gekozen RTO
Vernieuwen E-ID	L	H	H	K	48u

Stap 2: Vul de processenlijst in

Omvang impact	RTO	Prioriteit RTO	RPO	Afhankelijkheden	TKP/EP/ NP	

Stap 3: Definieer de benodigde middelen voor kritieke processen

Vereiste rollen	Vereiste tools en systemen	Vereiste Hardware	Vereiste werkruimte	Benodigde andere diensten of leveranciers	Contactpersonen met -info	

Stap 4: assessment van bedreigingen of risico's

Bedreiging of risicostatement	Kans of reden	Kans: L, M, H	Impact of beschrijving	Impact: L, M, H	Risico: L, M, H	Aanvaarden, verminderen, verwijderen, preventieve maatregelen?	

Lessons learned

- Geoblocking activeren op de firewall
- Buitenlandse IP-adressen blacklisten
- Multi-factor authenticatie
- Offline back-ups
- Service level agreement met softwareleverancier heronderhandelen, vragen sterkere garanties, bijv. inzake aansprakelijkheid.
- Toepassingen die lokaal draaien maximaal in de cloud zetten.
- Dankzij samenwerking met buurgemeente Scherpenheuvel-Zichem, die soortgelijke softwareoplossingen gebruiken, noodloket burgerzaken kunnen installeren. Interessant met buurgemeenten afspraken te maken rond het opzetten van noodloketten.
- **De gebruiker zelf is het grootste risico.** Dus stevig blijven inzetten op sensibiliseren van het personeel door phishing-acties en andere.
- Onze kwetsbaarheid én afhankelijkheid van technologie zijn zeer groot.



Vlaamse
Ombudsdienst