February 2020

What is the problem ?

Too late of missed detection of a Ransomware infection can shut down a business, sometimes permanently.

What is the problem with Ransomware ?

The latest generation of Ransomware slowly works its way through the infrastructure, waits until enough devices have been infected and then starts without being noticed to encrypt files.

Due to the number of devices involved in an attack, already encrypted files can be presented as normal without anyone noticing anything. This can take weeks, sometimes months.

As soon as a large enough number of files are encrypted the attack no longer presents normal files and the victim is presented with a Ransom note.

Antivirus solutions can often detect these attacks but never for 100%.
If something gets in without being detected it is really too late.

This is not scaremongering but unfortunately reality.

What does inspectOne solve ?

From the cloud detect a Ransomware attack in time in order for data to be recovered.

inspectOne is an Artificial Intelligent (AI) system using DeepMachineLearning (DML) which can detect all forms of Ransomware.

inspectOne works from the Cloud, files in our Cloud are detached from where they come from. Making any attack powerless.

Every file is inspected by the AI system of **inspectOne** and can be identified as Ransomware within 24 hours (often within 1 hour), information about this is send via email.

From a read-only area you can pick up a clean version. This is the last or the one before last (and then 14 previous versions and/or versions back in time for 90 days) guaranteed clean.

Due to the tight integration with our Cloud and **inspectOne** you can work directly from our Cloud and be assured of clean files.
If you don’t want to work online, at least use our Backup Online software once a day.

Should you become a victim of a Ransomware attack you only need 2 steps to get back up running again:

Step 1: Replace your hardware and/or re-install your workplace.
Step 2: Recover your files from our Cloud.

If you can't place all your files in our Cloud then make a selection of files who can at a different location, should Ransomware be active it will eventually reach this location after which **inspectOne** will alert you.

We also have the option to place an **inspectOne** scan machine (VDI) in your infrastructure.

What does **ECSystems** do to keep it clean and save ?

We could say that we keep everything up to date including patches, etc. but we're not. Everyone hopefully already does this.

What do we do extra to keep things save ?

- Not only networks are segmented, all application layers as well
- We use **inspectOne** also internally, if only one bit is in the wrong place the whole system is automatically and fully rebuild (this is done as a preventive measure once a week)
- Our Cloud storage systems are fully CIS hardening compliant
- We create for free extra backups up to 14 days, even backups of removed files up to 90 days
- Continues monitoring with DPI (wire data analysis), PRTG (scanning and behavior analysis)

We've been doing this for the past 15 years for small businesses with zero incidents.

During the beta period in December 2019 - January 2020 six small businesses managed to save themselves thanks to **inspectOne**, of the six, five businesses lost a maximum of 1 days' work.

Six small businesses with fully up to date software and the best antivirus…..

Let **inspectOne** take away the worry of continuity after a Ransomware attack.

Sign up via this document:
http://xfer.ecsds.eu/docs/Cloud_and_Backup_Online.pdf

inspectOne is part of our [**SafeGuard**] Suite
[**SafeGuard**]: The solution for safe Data Centers and VDI using Artificial Intelligence