DATA & SYSTEMS SECURITY

….. Hard times are a-coming for unsecured data

HIDDN PRODUCTS & OTHERS

Hiddn Technology

Confidential data residing on computers has become the

Major Security Challenge Of Public and Private Organizations

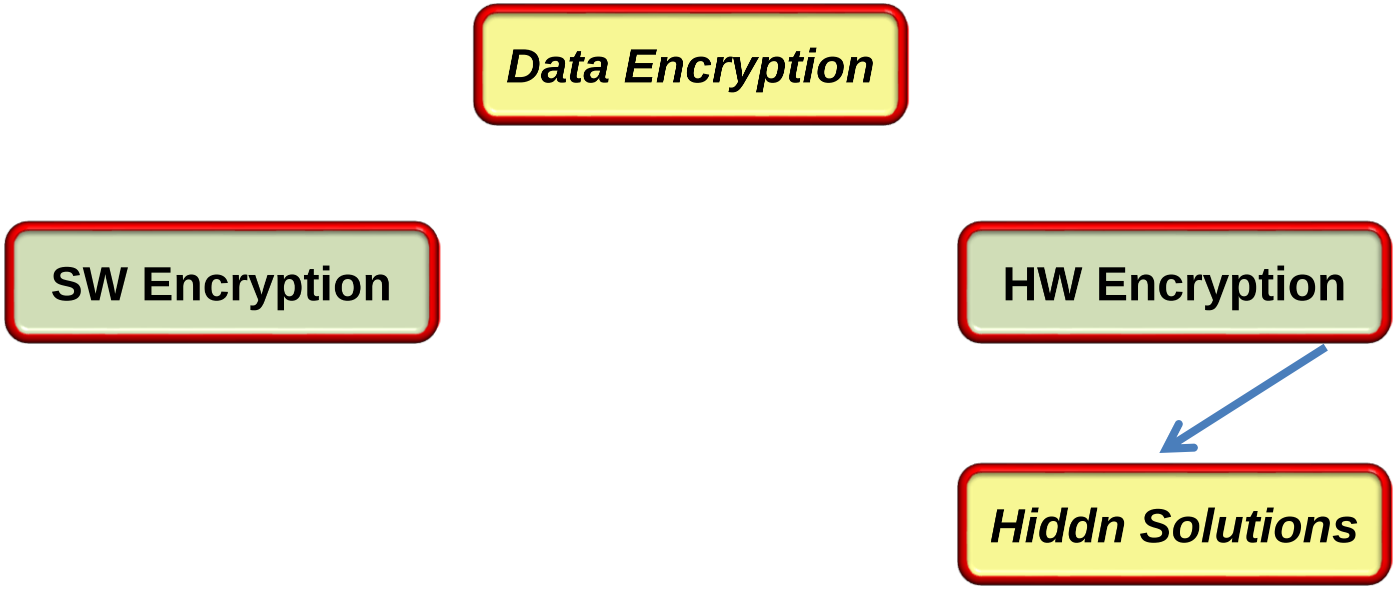
Critical Problems

Unexpected Consequences

Data Breaches May Have An High Cost

Hiddn Technology

What’s the logical solution?



Data Encryption

SW Encryption

HW Encryption

Hiddn Solutions

Hiddn Technology

Hiddn Key Benefits

Maximum Data Security

- Physical and logical barrier to intrusion and data theft
- Encrypted data can be decrypted only by owning the correct key
- No software associated with hiddn to install on the computer
- Cryptographic Keys never stored on the computer’s CPU, memory, or storage devices
- Cryptographic algorithms are inaccessible to processes running on the computer

Hiddn Technology

Hiddn Key Benefits

Performance

- The encryption hardware device is Self-Contained
- Real time encryption, independent from the computer CPU and Operating System
- No performance degradation

Hiddn Technology

Hiddn Key Benefits

Efficient Implementation

- Vendor Independent
- Operating System Independent
- No drivers required
- Transparent to user
- No user training, just insert the smartcard and enter the PIN
- Cost of data protection is lower than cost of remediation

Hiddn Technology

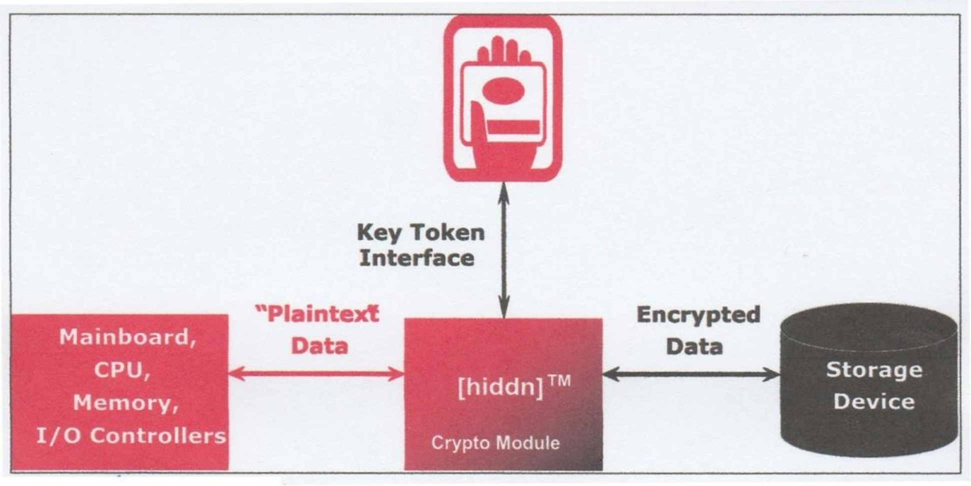
Hiddn Key Benefits

Encryption Methods

- The hiddn Crypto Module encrypts the entire disk
- No option of partial encryption
- The data encryption can never be turned off
- The laptop is inaccessible without the correct smartcard and the PIN
- Potential liability in case on stolen or lost laptop is limited

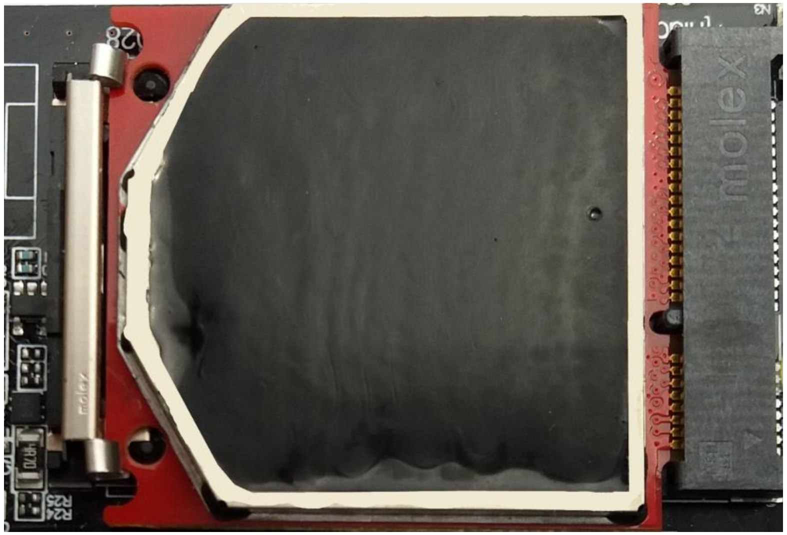
Hiddn Technology

Architecture



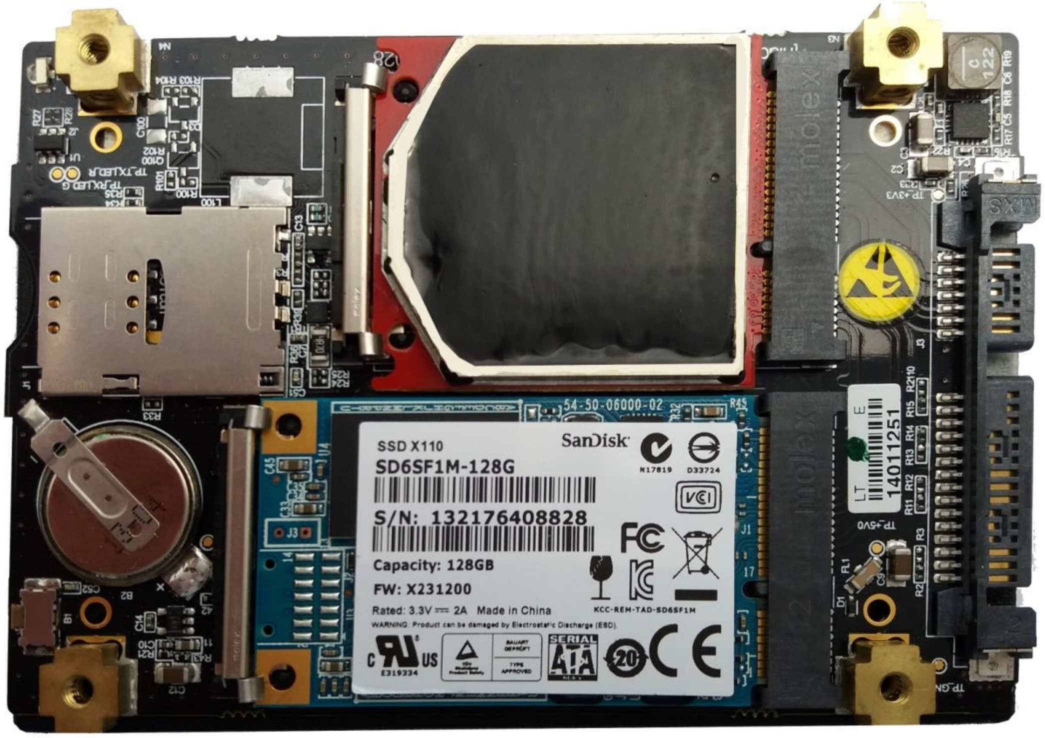
Hiddn Technology

Crypto Module



Hiddn Technology

Laptop 1 Plus



Hiddn Technology

User Authentication

- Supported 2-factor authentication mechanism
- Once the Smartcard has been accepted enter the PIN
- PIN code is maximum 16 digits
- The drive will never boot whitout the proper Smartcard and the PIN

The PIN can be modified

Hiddn Technology

Hiddn Certifications

- FIPS 140-2 Level 3 validated
- Based on Common Criteria EAL4/ISO 15408-3 (Certificate no. CCEVS-VR-050141)
- Based on Common Criteria EAL4+, augemnted with AVLA_VLA.3 (Certificate no. CCEVS-VR-06.0047)
- NATO Restricted
- Approved by Norvegian Security Authorities NSM
- Approved by Italian Security Authorities (DIS)
- Approved by Dutch Security Authorities (AIVD)

Hiddn Random Keys

KMS installation generates the primary Random Source

Secondary Random Source in the Smart Card

Nobody knows how the Random files are composed, even the Crypto Officer

Customized Hiddn Products

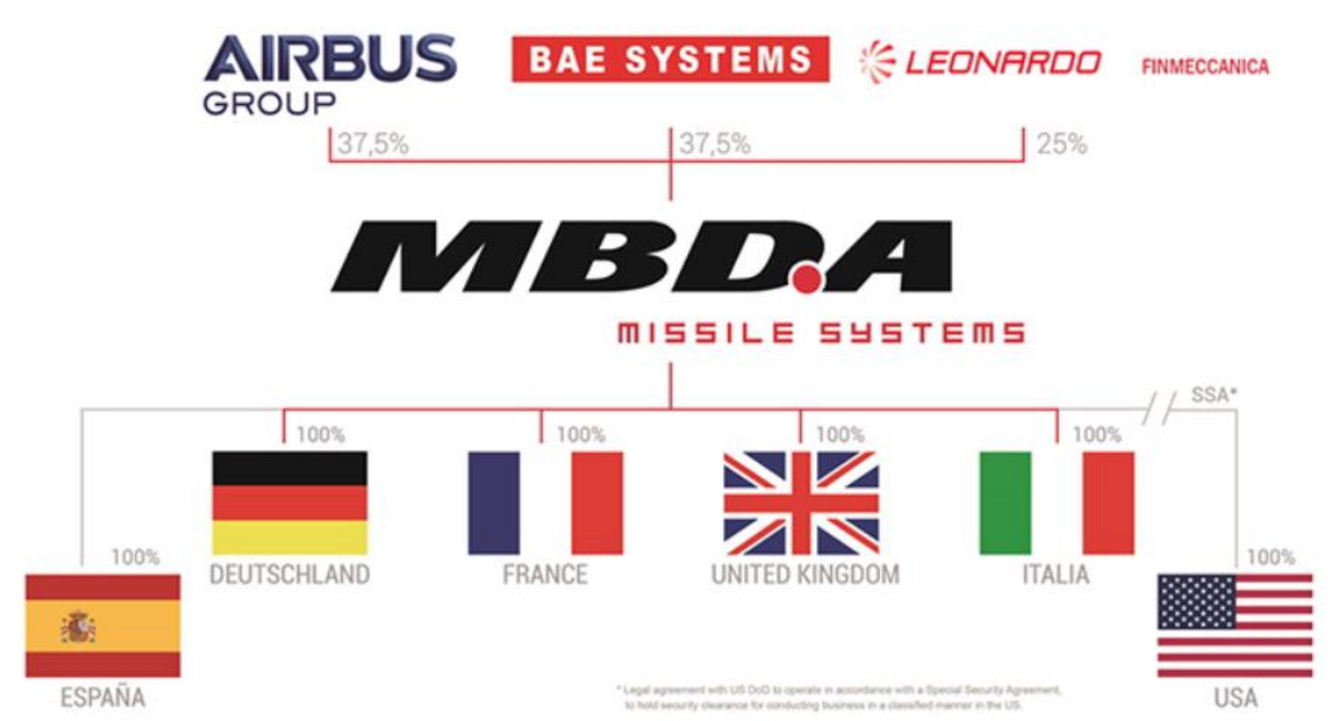
5 channel RAID storage – FW upgradable
Keys transferred in the air – wiped remotely

Customized Hiddn Products

esa

European Space Agency

Customized Hiddn Products



* Legal agreement with US DoD to operate in accordance with a Special Security Agreement, to hold security clearance for conducting business in a classified manner in the US.

Standards Hiddn Products

coCrypt

coCrypt + Xubuntu

Laptop1 Plus

PataDisk

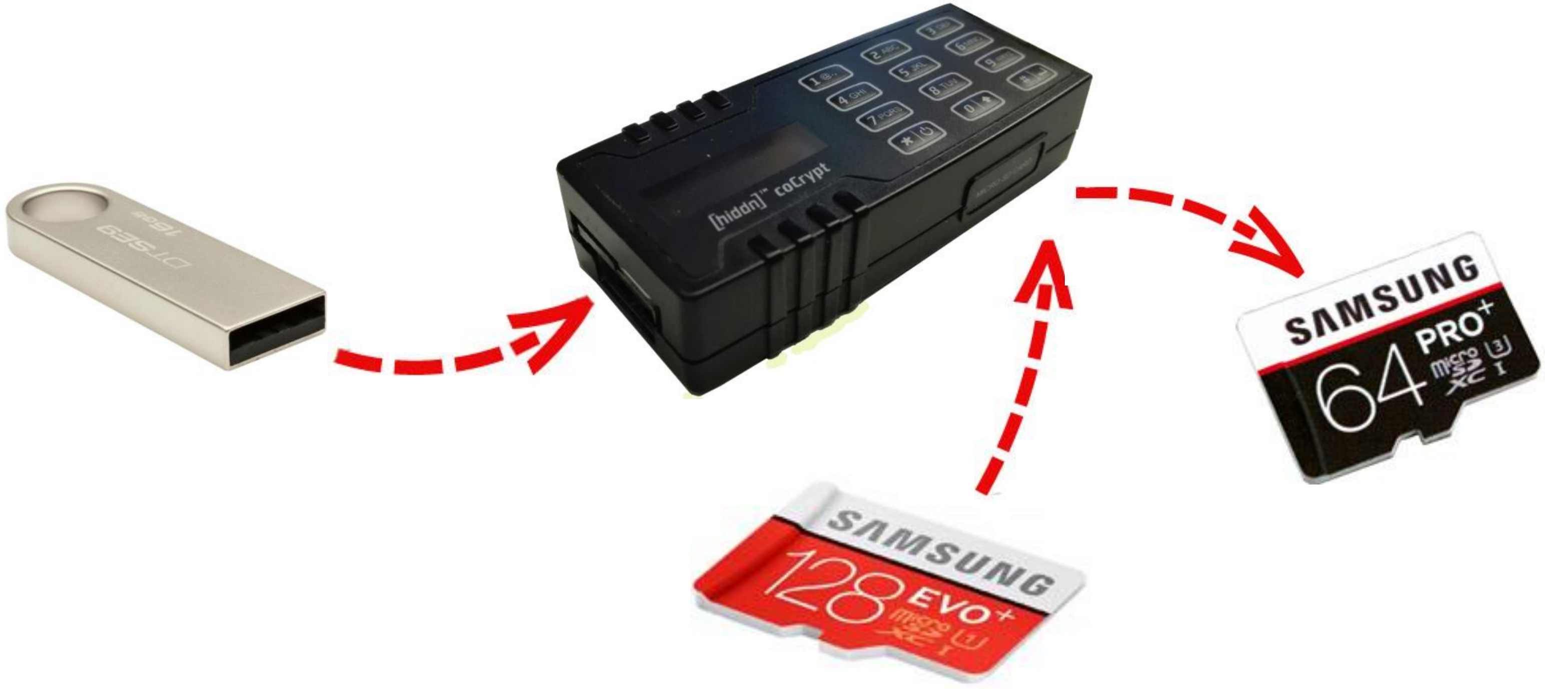
KryptoDisk

Hiddn coCrypt

Micro Smart Card Authentication + PIN

Capacity: 16, 32, 64, 128, 256 GB

Hiddn coCrypt



Hiddn coCrypt - Xu

Laptop *(without any Hard Drive)* **+ coCrypt** with bootable OS Xubuntu

+

Advantage: No trace or evidence on the Laptop
It seems you never used the Laptop

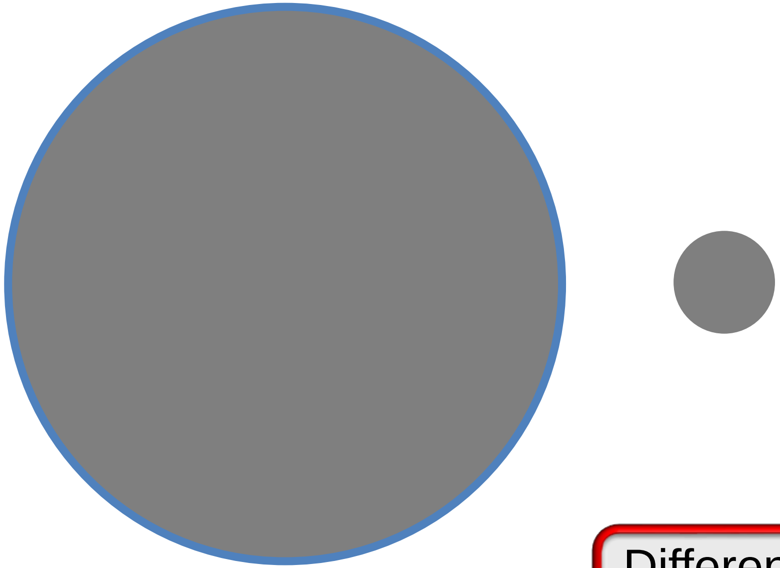
Hiddn Laptop 1 Plus

Smart Card Authentication via External USB Reader ACR 38U N1 + PIN

Capacity SSD: 128-256-512-1024GB

[hiddn] SSD + CM replacing the original laptop hard drive

Dual Systems AES 256



Hardware Hiddn Encryption

Software Encrypted Volume

Independent Systems

Different and separate Encryption Keys

Hiddn disk will protect data at rest. But after booting data become, that's visible and therefore vulnerable. An encrypted volume inside Hiddn disk will store data have to be protected when we are "online". We can create as many encrypted volumes we want or need.

Hiddn Pata Disk

Smart Card Authentication

Capacity 320 GB

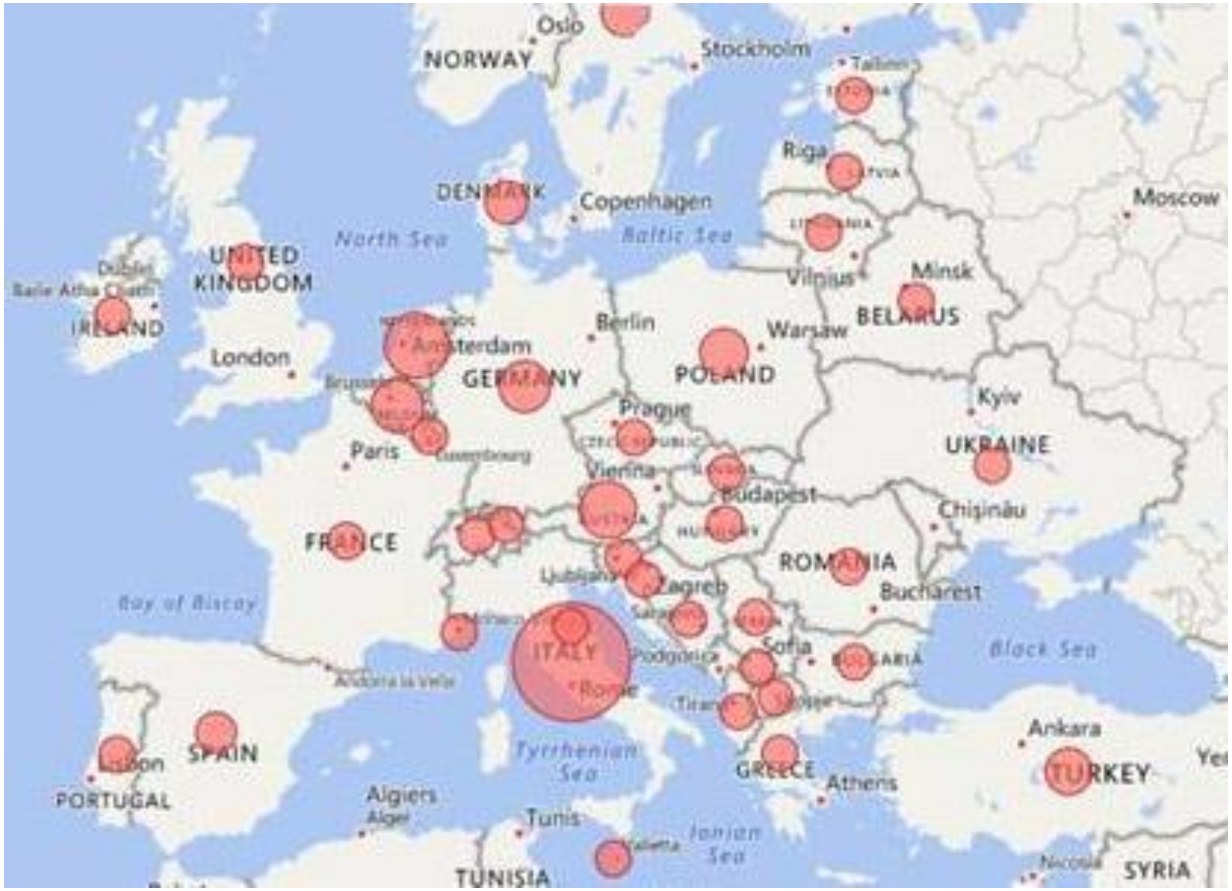
Hiddn Sata Krypto Disk

Smart Card Authentication + PIN

SSD: Capacity 128-256-512-1024GB

Rotating Disk: Capacity 1-2-3-4 TB

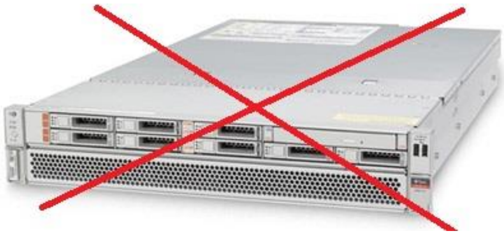
Ransomware: the daily danger

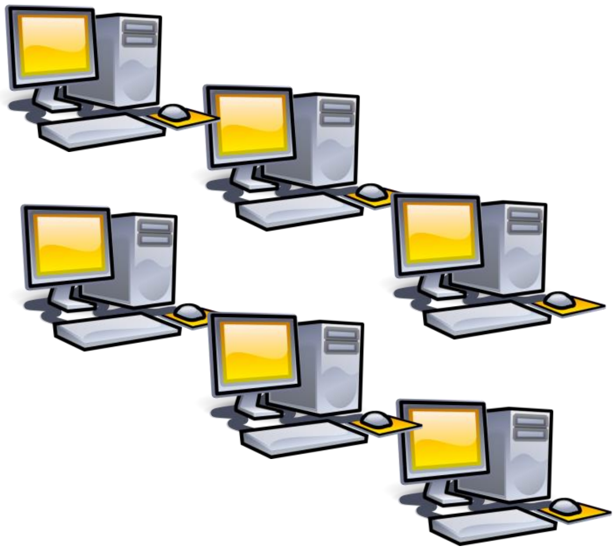


Software, Logical Procedures and Staff Training may block the ransomware action, or mitigate its damages.

Dangerous Configurations

OS + Applications
Data > Disk C
Backup > USB Disk
All plaintext





OS + Applications
Data > Disk C + Server
Backup Server > NAS
Backup PC > USB Disk
All plaintext

Secure Communications

1. Use asimmetric encription: PGP

2. Use symmetric encryption with shared password

3. Email draft with shared password

4. Attached file with extension

5. Steganography

6. Never send anything

E-mail Draft

Prepare an Email Account

Share the Password Account

Write the confidential message

Save it as draft

Make an innocent phone call

Your friend will read the message

Then he will send an innocent email

Or finally delete the draft