Sonpo

PREVENTION OF RANSOMWARE AND OTHER THREATS
RECOMMENDED PROCEDURES

E-MAIL PROTECTION CONFIGURATION

- Block executable content *(exe, js, vba, etc.)*, even if it is contained in archives *(such as exe in zip)* or documents *(vba, macro in doc)*.
    - to send such content, use only a dedicated channel, containing content checks and audit logs *(such as SOFiE)*, and block others *(Dropbox, OneDrive, Google Drive, MegaUpload, etc.)*
- Block encrypted files, which are often archives and Office documents. *(Their content cannot be checked and can be dangerous.)*
- Perform sandboxing of e-mail attachments and URLs passing through your e-mail gateway. *(using FortiSandbox for example)*.
- Implement the DMARC standard *(with reject policy)*. Plus optimally use the DNSSEC to secure DNS records.
- Use a high quality e-mail gateway with up to date commercial antivirus and antispam.
- Do not use secondary and other MX records bypassing the primary gateway with security checks.
- Only allow incoming SMTP connections to the e-mail server/platform *(such as Office365 or G Suite)* from the e-mail gateway, so that it is not possible to bypass the gateway and deliver unchecked e-mails directly.
- Block attachments with unusual archives *(allow only .zip, if possible)*. They may contain malware and might bypass some security engines.

PERIMETER AND LAN PROTECTION

- Appropriate network segmentation *(e.g. via VLAN)* into the smallest suitable subnets and segmentation firewall for filtering communication between these segments *(VLANs)*. Allow only necessary communication, block everything else *(not the other way around)*.
- Consistent use of demilitarised zones *(DMZs)* for everything accessible directly from the Internet. Also it should not be possible to access the LAN from the DMZs, only the other way around *(from the LAN to the DMZs)*.
- Always use a VPN for external access. Do not map ports from the Internet to the internal network. If a service requires it, it should be in the DMZ.
- Use an up-to-date, well-configured firewall with modern features *(IPS/IDS, web filter, application filter, antivirus)*.
- Use client isolation. Common function for better WiFi, but it is also suitable to use it for switches, i.e. "on cable" stations, if the switches support it *(to prevent the spread of malicious code between stations through local vulnerabilities)*.
- Block communication with known botnets and their C&C servers *(NGFW firewall functions)*.
- Implementation of a honeypot cooperating with the firewall to block detected attacks.
- Use additional lists with IP addresses to block known bad communication sources. We recommend using, for example, ones from NIC.CZ *(free)*.
- Perform inspections of HTTPS and other SSL traffic.
- Block communication with TOR type networks.
- Perform detailed network monitoring of the entire network.
- Block access to social networks, Dropbox type repositories and others.

Includes recommendations of NÚKIB

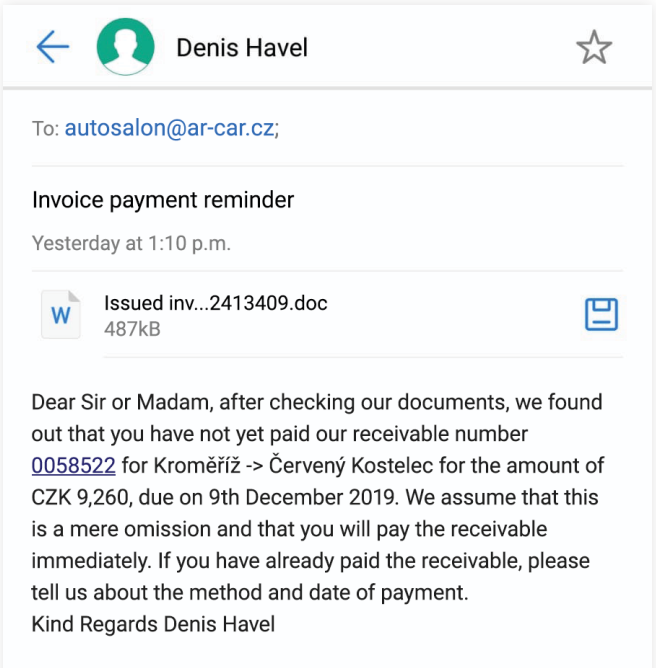
CONFIGURATION OF STATIONS AND WINDOWS SERVERS

- Do not use administrator or other privileged accounts for regular users and regular tasks.
- Do not store data locally on stations.
- Central installation of security patches and updates *(Patch management)* of all used products/software on stations.
  - Besides MS/WSUS, also solve updates of Acrobat Reader, Java, etc.
- Regular server updates.
- Use an updated antivirus system.
- Using domain policies *(GPOs)*:
  - Disable macros for Microsoft Office.
  - Optionally allow only secure limited features in MS Office.
  - Disable the use of custom USB drives and other external data carriers.
- Use only secure current browsers for the Internet.
  - If it is necessary to use obsolete and dangerous IE, then only for internal isolated applications.
- Restrictions for remote administration:
  - Disable RDP or enable it only from VLANs of IT administrators.
  - Run TeamViewer only when IT department requests it and then shut it down again.
- Use a smaller number of the same types of HW and SW configurations of stations. Have a fast automatic *(re)*installation *(reference clean image)* ready for these.
- Minimise access of own user devices *(BYOD)* to the network, e.g. allow only for dedicated VLANs.
- In addition to passwords, use MFA for administrator access wherever possible.
- Operate MS servers with Active Directory in their own VLAN. For the highest security the servers do not need to have direct access to the Internet and can be updated via WSUS.

BACKUP MANAGEMENT

- Regular checking of backups, including verification of backup functionality.
- Multiple versions of backups back in time, not just the last current copy of data. Example scheme: daily backups going back a week, weekly backups going back a month and monthly backups going back three months.
- At least two-stage backup, i.e. there must also be a secondary copy/ backup of backups. Preferably offsite *(in a cloud, another location, etc.)*. Secondary backups must not be directly accessible *(e.g. they must not be just another network drive)*. For particularly sensitive operations/data, there must also be offline backups *(e.g. tapes in a vault)*.
- So called 3-2-1 backup rule says, that there should be at least three copies of data on at least two different media and at least one in different location.
- Defined policy for data storage, backup and recovery – where is what data, e.g.:
  - station – no data – recovery by *(re)*installation of reference image
  - servers
    - SQL – a consistent database backup is required with dedicated tools and procedures *(dump database)* – recovery = installation of a new empty server *(ideally automatically from the image)* and loading of database data from the DB backup
    - File server – versioning, copies of files, etc.
    - Virtual servers – backups usually in the form of snapshots of the entire VM for fast recovery
  - disk arrays, NAS
  - about clouds and data in them *(files, databases, services)*.
- Backups should be encrypted as they usually contain sensitive data.

Example of a phishing email with a compromised .doc attachment:



PASSWORD MANAGEMENT AND POLICIES

- In general, it is important to ensure that weak passwords are not used without an additional factor, especially where their remote misuse is possible.
- It is not possible to leave the default accounts and passwords set from production/installation/ reset, not even on devices only in the internal network.
- Use accounts with the lowest suitable permissions for your work.
- Use a unified MFA solution wherever possible.

1. USERS

- Ordinary users cannot reasonably be required to use complex difficult to remember passwords, change them regularly, not write them down, use a different password for each service, etc. A good solution must therefore be one that ensures a good level of security even without meeting such requirements.
- Make maximum use of the "Single Sign On" *(SSO)* system, where a single user account *(e.g. in Active Directory)* authenticates the user to all necessary services. This has the following advantages:
  - a better password can be used when the user just has to remember one
  - the account can be deactivated, password changed, etc. in one place.
- If possible, supplement the use of a password with a second factor *(MFA - mobile phone, chip card, Yubico, etc.)*. The password can then be simpler as it itself is not sufficient for authorisation.
- Do not require regular password changes. This is an outdated concept, which leads to the fact that passwords are then weaker, systematically deducible or written by users in inappropriate places *(papers, unencrypted files, etc.)*.

2. IT STAFF

- Administrators and IT professionals typically need to use a large number of accounts in different services and devices where it is not reasonably possible to consolidate them under a single SSO system. Additionally, some accounts often need to be shared among multiple people. In order to maintain a good level of safety, it is necessary to:
- Use a suitable password manager *(e.g. BitWarden, LastPass, KeePass, etc.)*, thanks to which:
  - Each account can have a unique complex randomly generated password;
  - You can create containers for shared passwords and assign authorisations to them, and you can easily change your shared password without having to let everyone who uses it know;
  - It is possible to determine and check or require the implementation of various policies for working with passwords *(strength, uniqueness, whether it is compromised in a known password leak, etc.)*;
  - Passwords are encrypted, secure and stored in a place dedicated for this purpose;
  - Access to passwords can be secured by high-quality multi-factor authentication;
- Passwords can be used offline/backed up in case the password manager does not work.

3. EXTERNAL SUPPLIERS

- For external suppliers, use systems for managing privileged accounts *(e.g. CyberArk)*.
- Use specialised jump servers for access *(SSH, RDP, ...)*.
- Use a universal MFA solution for authentication.

OUR SERVICES AND SOLUTIONS

- Security audits, analyses and consultations
- Penetration tests *(internal and external)*
- Configuration audits
- Regular health checks
- Expert consultations on ransomware protection
- Analysis of compliance with ZoKB, ISO 27000 and GDPR
- Training of administrators and users
- Solutions of emergency situations in cyber incidents

Sonpo

SONPO, a.s. | Klapkova 546, 182 00, Prague 8
www.sonpo.eu | sales@sonpo.eu