Checklist for Security Measures to Prevent Ransomware Attacks

Non-official convenience translation – prepared by Osborne Clarke

Checklist for basic technical and organisational measures pursuant to article 32 GDPR to safeguard against ransomware attacks

1. IT Landscape

A complete and up-to-date overview of all IT systems and IT components (such as clients, servers, firewalls, switches, VPN endpoints) used in the own operation is available (IT inventory, network plan). Proper network and system management is in place for this purpose (including IT network separation, securing remote access, secure basic configuration of systems and applications), which includes the documentation of the IT network as an essential component. Aspects of secure mobile working (e.g. in the home office) are also sufficiently illuminated in the treatment of the system landscape (such as connection of telework places and other mobile clients, mobile device management, regulations on Bring Your Own Device, release guidelines).

	Measure	**Why should this measure be implemented?**
☐	Complete and up-to-date list of all existing PCs and notebooks including operating system and operating system version is available.	Prerequisite for effective patch management.
☐	Complete and up-to-date list of all work smartphones, tablets and other mobile devices including operating system and operating system version is available.	Prerequisite for effective patch management.
☐	Complete and up-to-date network plan with all internally and externally operated IT systems including active and passive network components (e.g. switches, firewalls, VPN appliances) including network segmentation, if any, is available.	Prerequisite for effective patch management.
☐	Internal network areas of different security levels are separated by means of firewalls.	Making it more difficult to/prevent the spread of malicious code or attackers within the network.
☐	Servers that can be reached via the internet, such as mail servers, web servers or VPN endpoints, are located in their own internal network segment, which is protected from the internal network by means of a firewall (demilitarised zone - DMZ).	Preventing attackers who may briefly take over such a service from easily accessing other internal systems or at least attempting an attack.
☐	Connection of mobile workstations (e.g. work notebooks, work smartphones) via the internet is done via encrypted and cryptographically authenticated connections (e.g. encrypted VPN with authentication by means of strong passwords and cryptographic client certificates).	Attackers should not be able to access the company network solely on the basis of stolen user names/passwords.

	Measure	Why should this measure be implemented?
☐	Programmes downloaded from the internet cannot be executed without user interaction.	To prevent the automated execution of malicious codes downloaded from the internet after a Microsoft Office macro has been activated unintentionally.
☐	Programmes without valid signing of the authenticity by the operating system cannot be executed.	Malware mistakenly downloaded by the user from the internet is not executed.
☐	No private devices in the home office are fully connected to the company network (only company-administered terminals should be used).	The level of protection of private end devices cannot be guaranteed by the controller.
☐	Company smartphones and tablets are managed via a mobile device management solution.	Prerequisite for effective patch management and data deletion in case of loss.
☐	The installation of software on a PC is only possible with admin rights (by the administrator).	To prevent users from accidentally installing malicious codes disguised as normal software.
☐	Browser plug-ins (e.g. Flash, Java) are only installed if an (older) application makes this absolutely necessary.	Many browser plug-ins have security vulnerabilities that can be exploited while visiting a website (so-called drive-by attacks).
☐	Scripts such as JavaScript or Visual Basic are only left executable by the operating system (not by the browser, here at least JavaScript is usually required) if (older) software absolutely requires this.	Some malware comes as a script file in the email attachment and can still be prevented from executing by deactivating it on the operating system side if the user accidentally clicks on it.
☐	Microsoft Office packages should be configured to execute only signed macros.	Malware often comes in the form of prepared Office documents such as Word or Excel. These do not have signed macros and can thus be prevented from being executed.
☐	Checking whether the execution of programmes is only possible from specified directories (whitelisting).	Prepared emails often do not contain the malicious code itself, but small programmes that automatically download it from the internet. The malware downloaded in this way is stored in specified directories of the operating system and can be prevented from executing by releasing valid - and in this case different - directories.
☐	A spam and anti-virus filter is used on the email server.	This allows already known malware to be detected and suspicious emails to be treated separately.

	Measure	Why should this measure be implemented?
☐	Emails with dangerous file attachments such as executable files, ZIP archives encrypted with a password or Microsoft Office documents with macros are moved from the mail server to a quarantine folder for analysis.	Such emails often contain malicious code or small programmes that are supposed to download malicious code. Since these are not frequent by now, a manual analysis by the IT administration can be carried out well.
☐	The email server is configured in a way that emails from internal senders, but which are to be delivered from outside the company, are blocked (anti-spoofing).	This attack is not unusual, e.g. to entice employees to click on a link contained in the email (which leads to malicious code). Since such emails always come from "outside", it is factually impossible (except for email distribution lists, which should then be tested) that they have an internal sender address and are not forged.
☐	Administrators have two user accounts: One for pure administration tasks and one for other activities such as reading emails or surfing the internet.	Malicious code always executes with the user rights of the person who (inadvertently) contributed to its activation. In this way, it can at least be prevented that the malicious code is immediately executed with (local) privileged administrator rights.
☐	A different and strong (at least 16 digits) password is used for the local administrator/root account on each PC/server	If an attacker/malicious code is able to obtain the local administrator account of a computer, this does not immediately allow lateral movement across the entire network.

2. Patch management

There is a regulated update process for all IT systems and applications used, including the corresponding documentation for the version overview and updates. Information on security vulnerabilities of the components used is regularly evaluated so that important security updates can be applied without delay. The company's own server landscape is checked with regard to patch level and vulnerabilities. In particular, the servers connected to the Internet are checked regularly (including ongoing monitoring). Preparations for non-patchable security gaps (zero-day exploits) have been made in order to be able to react appropriately and promptly in the event of an emergency.

	Measure	Why should this measure be implemented?
☐	All PCs and notebooks are configured in a way that software updates of the operating system are automatically installed.	Security gaps are closed immediately and can no longer be used by attackers.
☐	If software updates of the operating system are carried out via a separate software distribution (e.g. WSUS), this must be configured in such a way that	Security gaps are closed immediately and can no longer be used by attackers.

	Measure	Why should this measure be implemented?
	security updates are automatically loaded by the manufacturer of the operating system and immediately made available for updates to all PCs and notebooks.	
☐	Only operating systems for which the manufacturer provides security updates are used.	Otherwise, security gaps cannot be closed at all.
☐	There is a complete list of the application software used on all PCs and notebooks, including the software status.	Prerequisite for being able to organise the installation of software updates.
☐	Application software on PCs and notebooks is configured in such a way that software updates (at least security updates) are applied automatically, if this is possible.	An attack by means of known security vulnerabilities (e.g. browser, PDF reader) can be prevented.
☐	If application programmes cannot be updated automatically, it is ensured that they are updated to the latest version at least once a month.	An attack by means of known security vulnerabilities (e.g. browser, PDF reader) can be prevented.
☐	Only server operating systems for which security updates are provided by the manufacturer are used.	Otherwise, security gaps cannot be closed at all.
☐	It will be checked for all servers to what extent they can be configured in such a way that security updates can be applied automatically.	To prevent attackers from successfully attacking internal servers by exploiting known security vulnerabilities and thus misusing them for further propagation in the local network.
☐	For all servers for which no automated import of security updates is possible due to risks of possibly unstable server states, security updates are applied manually without delay after tests. Critical security vulnerabilities are applied within a few days unless equivalent other protective measures are taken.	To prevent attackers from successfully attacking internal servers by exploiting known security vulnerabilities and thus misusing them for further propagation in the local network.
☐	Security updates of all network components, especially firewalls and VPN appliances, are applied immediately with high priority.	Especially in the case of central systems accessible via the internet, a successful attack means an immediate failure of critical protection components.
☐	There is up-to-date and complete documentation on which PCs, notebooks, servers, network components, etc. are updated automatically or manually. In the case of non-automatic updates, the respective IT systems and their software versions are recorded.	Only through minimal and lean documentation can the effectiveness of an update concept be ensured and controlled.
☐	Security updates for work smartphones and work laptops are rolled out immediately via a mobile	To prevent attackers from successfully attacking mobile devices by exploiting

	Measure	Why should this measure be implemented?
	device management system. No mobile devices are used for which there are no (more) security updates.	known security vulnerabilities and thus gaining access to the corporate network.

3. Backup concept

An effective backup concept is in place that either implements the idea of the "3-2-1 rule" (three data copies, two different storage media, one of them at an external location) as needed or that takes into account another effective approach specifically geared towards ransomware threats. Backups are automated on a regular basis. Tests are carried out to ensure that all relevant data is included in the backup process and that a recovery works. The backup concept is thus regularly checked with regard to its effectiveness. Measures are also taken to ensure that data backups cannot be encrypted.

	Measure	Why should this measure be implemented?
☐	Carrying out backups according to the 3-2-1 rule: three data storages (incl. original data), two different backup media (also "offline" such as tape backups) and one of them at an external location or comparably effective backup mechanisms with regard to ransomware attacks.	In the event of a ransomware attack, the (personal) data and the affected IT system can be restored.
☐	At least one backup system cannot be directly encrypted by malicious code (e.g. special data backup procedure such as pull procedure of the backup system, air-gap disconnected (offline) after completion of the backup process or write authorisation to backups only from specified programmes).	Many ransomware attacks attempt to also encrypt the backup systems or delete the backups before encrypting them. Solutions targeted at ransomware attacks are intended to minimise risks regarding active attempts to delete the backups.
☐	There is a documented regulation as to which data from which servers or PCs/notebooks have been included in a backup concept.	To ensure that all relevant (personal) data is also covered by a backup solution.
☐	A threat simulation was carried out to see how the entire IT system could be restarted in the event that all internal and external servers were no longer functional due to full encryption.	Preparation for the worst case to be able to check whether all necessary data are included in the backup.
☐	Regularly check that at least one backup is carried out daily.	A backup must be carried out daily - it must also be ensured that the backup works.
☐	Regular tests to ensure that all relevant data is included in the backup process and that the recovery works.	To prevent the situation that, in the worst case, it is discovered that, for example, a backup medium is defective or that information required for a system restoration is not contained in the backup.

4. Checking the data traffic

Calls at the internet transition point are checked by us in such a way that network activities from the internal network to known compromised external servers can be detected (e.g. at the firewall the Indicators of Compromise, IoC). There is blocking, logging and alerting on this, along with daily updating of the IoC lists by appropriate sources. There is also a logging and analysis concept (handling of error messages, protection against manipulation, logging, monitoring and securing of log files). Firewall systems are regularly checked for proper configuration.

	Measure	**Why should this measure be implemented?**
☐	The central internet transition point from the internal network to the internet is secured by means of a firewall.	Minimum standard for securing confidential networks against the internet.
☐	In addition to/as part of the firewall, http traffic is routed via a web proxy. Network traffic of other protocols to the internet is blocked by the central firewall as standard and only released in individual cases and documented.	Prerequisite for analysis of possible malware network traffic.
☐	The web proxy component filters accessed websites with regard to known and daily updated endpoints that are used as (mostly hacked) servers for the delivery of malicious code (so-called Indicator of Compromise, in short: IoC) and blocks as well as logs such calls.	Malicious code is usually "delivered" in several steps, which can sometimes be prevented in this way.
☐	A logging of data traffic to the internet based on external IP addresses and data volume for up to 90 days takes place with the aim of evaluating possible irregularities after an incident. These logs should be encrypted in order to prevent misuse and to ensure that they are used for the intended purpose in accordance with data protection law.	If there is a suspicion of data exfiltration after a ransomware attack, this can be used to create an indication of whether data exfiltration has taken place or not. The IP addresses can then be handed over to the police for their investigations.

5. Awareness and Authorisation

Employees are trained regularly and appropriately on attack methods in line with the publicly known threat situation. The focus is on current social engineering techniques and forged emails, which may also have a connection to known email correspondence, some of which is the staff's own. Those trained are instructed on what behaviour is appropriate (e.g. no clicking on foreign links, no opening of certain files, no activating macros). Employees are provided with a selection of secure authentication procedures for working on the terminals (including strong passwords with at least 10 digits for standard passwords and at least 16 digits for administrative passwords, two-factor solutions, especially for administration, no reuse of local administrative IDs on Windows computers). The roles and authorisations are set up according to the least privilege principle.

	Measure	Why should this measure be implemented?
☐	Regular training of employees regarding current and frequent cyber-attacks (e.g. once a year).	Criminals use social engineering attacks to obtain important information for downstream cyberattacks. Accordingly, it is important to explain the "human security factor" to all employees in appropriate training courses.
☐	Consistent instruction of new employees on the proper handling of IT components and behaviour in the event of social engineering attacks.	Social engineering attacks continue to cause high damage.
☐	Raise awareness of IT risks among new employees before they start processing data (e.g. also for temporary staff).	Safety-related misconduct by employees is often based on a lack of awareness and information in advance.
☐	Presentation of the process of social engineering attacks to raise awareness among employees (e.g. possibility of manipulating telephone numbers).	Social engineering attacks continue to cause high damage - the presentation of concrete processes improves the employees' knowledge.
☐	Information to staff on reporting channels (e.g. by the CISO or DPO) and responsibilities.	An appropriate response to security-related misconduct is a crucial factor for an effective and timely response to a cyber-attack.