REDSOCKS
malicious threat detection

Mandatory data breach reporting

Technically compliant within 48 hours with RedSocks

The Dutch law making it mandatory to report data breaches comes into force on 1 January 2016. This means that from 1 January, all public and private companies which hold personal data will be obliged to report the theft, loss or misuse of any such data.

Report data leaks within two days!

The guidelines which have now been published stipulate that incidents must be reported within two working days of becoming aware of them. On average malware is present for 229 days before it is discovered. Because malware can create a data breach, detection has become even more relevant. So now it is not only important to comply with the new regulations because of security, but also to achieve compliance. Alongside the fact that the regulator has now acquired extended fining powers, it's important for every organization to get everything under control as quickly as possible, to be able to limit as much financial damage as they can.

What does the Mandatory Data Breach Notification Act involve?

The Mandatory Data Breach Notification Act augments the existing Personal Data Protection Act (WBP in its Dutch acronym). The WBP requires organisations to report security incidents involving personal data. Other countries such as Germany, the United Kingdom and the United States already have such legislation. The European Union has also announced imminent legislation, namely the EU General Data Protection Regulation, making it an absolute obligation to report breaches. You might perhaps wonder exactly what constitutes a data breach. Dutch Data Protection Authority the DPA has drawn up the following legal definition.

Data breach

"A data breach involves access to personal data or the destruction, alteration or release of data without this being the relevant organisation's intention. Thus a data breach involves not just the release (leakage) of details, but also any unlawful alteration of data. We refer to a data breach if there has been a violation of security (as intended in Article 13 of the Personal Data Protection Act). In a data breach, personal data is exposed to loss or unlawful alteration – thus to that which the security measures are intended to protect against."

The Mandatory Data Breach Notification Act means that ransomware must also be reported. Ransomware causes files to become inaccessible to their rightful owners by blocking them. Ransomware is a broad concept, making it unclear when ransomware must be reported.

The Dutch Data Protection Authority (DPA in Dutch) has drawn up the following guidelines to impart clarity to this. If as an organisation you are certain that personal data has been involved in a ransomware/malware case, the DPA advises that it should be reported, to avoid any considerable subsequent fines.

How do data breaches occur?

Data breaches may occur in a number of ways, including:

- A lost USB stick;
- A stolen laptop;
- Intrusion by a hacker;
- Sending out an e-mail in which the e-mail addresses of all the recipients are visible to everyone else;
- A malware infection;
- A disaster such as a fire in a datacentre.

Suitable technical and organisational measures

The Mandatory Data Breach Notification Act also requires personal data to be secured in a suitable manner. Article 13 of the WBP:

"The responsible party shall implement suitable technical and organisational measures to protect personal data against loss or against any form of unlawful handling."

You might ask what steps you need to take to comply with these conditions. Particularly, too, because the legislator provides no specific details about the way such protection must be achieved. The organisation itself is expected to be able to show that its security does actually work. Ultimately you want to avoid any possibility of incurring a fine to a maximum of €810,000 (or 10% of annual turnover) or that your company suffers any reputational damage. RedSocks and its partner Duthler Associates have thus drawn up a step-by-step plan to ensure that your company has implemented the necessary technical measures within 48 hours, and that in combination with existing and other supplementary measures, it can present a demonstrable compliance trajectory to the regulator. You will find the step-by-step plan below.

What does RedSocks Malicious Threat Detection do?

RedSocks Malicious Threat Detection is a network appliance which analyses digital traffic flows in real-time. Mala fide traffic is detected by using NetFlow and IPFIX. The RedSocks MTD is fed continually by the Malware Intelligence Team which compiles the risk lists and algorithms. Heuristics is also used, meaning that the RedSocks MTD can itself generate new risk lists automatically.

RedSocks believes corporate privacy to be paramount. Our systems and the flow monitoring systems have thus been developed to secure privacy to the utmost. RedSocks thus monitors flowdata (metadata) rather than content, so that sensitive corporate data always remains confidential.

The RedSocks MTD can store more than 12 months' data in a forensic manner, making you instantly compliant with the legislation. Using NetFlow and IPFIX makes the RedSocks MTD extremely scalable, so that the growth of your company is not a problem.

Compliance trajectory with RedSocks Malicious Threat Detection

Step 1

It's advisable to screen contracts with suppliers, where some can be qualified as handlers, and to amend them where necessary in accordance with the Mandatory Data Breach Notification Act. In collaboration with First Lawyers, Duthler Associates has developed a resilience check and processor agreements tailored in conformity with Article 14 of the act. This approach is aimed at limiting any liability and cost risks for the parties involved.

Step 2

Ensure that you are familiar with your responsibility and liability domain, and document all handling of personal data. That is not of itself sufficient however. You want to be able to arm yourself against any questions from involved parties and regulators. Then ensure there are effective internal checks.

In collaboration with Duthler Associates, SBR Powerhouse has developed the SBC Management System. The system helps organisations to acquire both an insight into, and overviews of, all handling related to processes and information systems, and is also aimed at maintaining this. The system thus establishes at any given time that the internal controls have functioned effectively. This can occur automatically based on taxonomies. The rights of those involved are facilitated, and the obligations of the responsible parties can be fulfilled. Naturally the Data Breach Notification Act is supported.

Step 3

Confirming the effective operation of the relevant management and security measures to protect privacy is not an easy task. With the application of RedSocks Malicious Threat Detection, data breaches in the technical information infrastructure can be tracked down, and evidence is presented of the effective operation of the measures in the network. RedSocks and SBR Powerhouse work in conjunction and have developed a taxonomy making it possible to incorporate the findings and the proof of adequate operation of RedSocks in the SBC Management System. This enables companies and institutions to take a significant step towards managing the liability and cost risks arising from the data breach reporting obligation.

Risk lists and algorithms are being updated continually to ensure that data breaches are always detected at lightning speed. This also makes you instantly compliant with the requirement that your measures must be demonstrably effective. The RedSocks MTD is fed with new lists every hour.

Help! There's a data leak, what now?

You do everything to prevent data breaches. But if one should occur despite all this, it must be tackled adequately and efficiently. Incidents must remain incidents and not turn into a crisis. In the case of a data breach you must notify the regulator within two working days. The regulator must be notified of the following issues:

- The nature of the data breach;
- The suspected scope of the data leak;
- The suspected nature of the damage ;
- The efforts undertaken to repair the damage;
- Advice issued to involved parties to cope with any effects to their own interests as far as possible;
- Identity and contact details of the official responsible for data protection (FG in Dutch) ;
- Measures to prevent any future data breaches.

In a short time information must thus be collected to be able to analyse whether the regulator and/or involved parties must be notified. To deliver this information successfully, preparatory and response plans must be in place to have the legally-required information available within a very short time, to repair the damage and to tackle the intrusion.

If a data breach occurs, you must convene the data breach emergency team as rapidly as possible. You determine what processing and which individuals could be or are affected. You determine which entities or organisational units of the corporate family are involved. You determine which handlers, suppliers or subcontractors play a handling role, on the basis of which agreements. If you use SBC Management System you are able to have this information on the table quickly.

You collate the required information, and notify the regulator and any parties who may be involved within the stipulated time.

Note : being prepared to deal with and settle a data breach is not an issue for the ICT department or operational management, but is in fact a corporate issue which must at the very least involve legal affairs, compliance and communication.

After a data breach

Once you have reported to the regulator and/or involved parties within two working days, you must then document the data breach which has or has not succeeded, related to the handling, the processes and the information systems. This applies to all elements of the information which you must provide to the Data Protection Authority (DPA).

You can also do this with the SBC Management System. This then enables you to demonstrate compliance with the law. You need this for the regulator and the annual compliance review. Should a fine be imposed, it strengthens your position with the regulator. It also strengthens your position with the parties involved should they file damage claims against you.

Are you interested?

Then please get in touch with us without any obligation, by e-mailing **info@redsocks.nl** or calling **+31 (0)55 36 61 396**.

REDSOCKS

RedSocks is a Dutch company specialised in malware detection. RedSocks supplies *RedSocks malware threat defender* as a network appliance. This innovative appliance analyses digital traffic flows in real time based on the algorithms and lists of malicious indicators compiled by the RedSocks Malware Intelligence Team. This team consists of specialists in identifying new threats on the internet and translating them into state-of-the-art malware detection.

REDSOCKS
malicious threat detection

www.redsocks.nl

Laan van Nieuw Oost Indie 133F - 2593 BM Den Haag , The Netherlands • **Tel** +31 (0)55 36 61 396 • **E-mail** info@redsocks.nl • **Website** www.redsocks.nl