Zomerlust
Systems
Design
(CK1997/001363/23) trading as ZSD

Unit D11,
Clareview Business Park
236 Lansdowne Rd

info@zsd.co.za
http://www.zsd.co.za

P.O. Box 46827
Glosderry, 7702
South Africa

☎ +27-21-683-1388
📠 +27-21-674-1106

3 Apr 2019

ZSD Security Check List

This check list is based on ZSD's experience and feedback from our clients, coupled with industry best practice advice from organisations like US-CERT the United States Computer Emergency Readiness Team (https://www.us-cert.gov/). These are basic guidelines. Not all items will apply to all organisations and some organisations will require more advanced considerations.

- **Up to date, licensed software:** All software should be up to date with valid current licences. This includes Windows, Java, Adobe, Mozilla etc. This also applies to websites that use content management systems like “Wordpress”. Most malware and viruses exploit known vulnerabilities in popular software. Industry experience is that many exploits occur after security updates for the targeted software have already been released, but the updates have not been installed on the victim’s computer.

- **Anti-virus software with up to date support:** Anti-virus software can pick up and block a lot of common malware. However it is important to understand that anti-virus software is reactive. It only blocks malware that has already been identified and for which signatures have been circulated. It provides no protection against “zero day” attacks and targeted attacks aimed at a limited audience using variations of malware which do not match known signatures.

- **Backups:** Encryption attacks are rife. Irrespective of what defences an organization may have in place, one must assume that it is only a matter of time before one falls victim to such an attack. The only remedy is a valid, working backup.
  - Backups should be the responsibility of a senior manager.
  - Backups should be checked and verified on a regular basis.
  - Backups should be audited to ensure that all valuable organisation data gets backed up, especially when new software has been commissioned.
  - Special consideration should be given to special software like databases and mail systems which may not be properly backed up by a normal file backup.
  - Backup storage should be beyond the reach of the attacker and it should contain historical data so data can be rolled back to a date prior to an attack.
  - Consideration should also be given to the user friendlessness of a data restoration event. It may take days to download a hard drive's worth of data from a remote backup service.
  - Multiple redundant backups can be useful.

- **Non-Trivial passwords:** Dictionary attacks are rife. Weak passwords will get exposed, it is only a matter of time.

- **Exposed Remote Desktop logins:** We see continuous scanning of all IP addresses for Windows Remote Desktop service. If this service is exposed on a public IP address, via port forwarding or similar, even on a non standard port, it will be discovered by attackers. They will then turn their attention to known exploits and dictionary attacks. Thus computers hosting the Remote Desktop Service, exposed to the internet, must have secure software and ALL the accounts on that server must have strong passwords. Connection rate limiting on the firewall can provide some protection but a two stage login process using a VPN is recommended.

- **Stored Passwords:** If passwords are stored on a computer which then gets compromised, all the systems accessible via those passwords are also vulnerable. Common malware searches the victim’s hard drive for stored Remote Desktop and FTP credentials and then attacks those servers.

- **Sensible management of privileges, access control and permissions:** For example, IT support personal should not use Administrator accounts for tasks like browsing and reading e-mail. File servers should not allow anonymous write access, without authentication.

- **Phishing:** We regularly see carefully crafted “phishing” messages that use social engineering to trick a user into installing malware on their computers or releasing their login credentials. Stolen credentials are used for things like banking fraud or sending spam from the victims e-mail account. Be very careful with “strange” messages. Do not click on embedded links nor open attachments from unexpected messages. These messages may appear to originate from a known source but in fact be a forgery. If in doubt, check first.

- **Banking Fraud:** This is a social engineering problem rather than a computer one. This is still rife and the extent of the problem is not fully acknowledged by the local banking industry. Organisations should have procedures in place to verify account details before large payments are made into previously unknown accounts. Ideally the party making the payment should make a phone call to the payee and speak to someone that they have dealt with before to confirm the bank account details, before releasing funds. Beware of documents like “proof of payment” and “proof of account” as these are readily forged. Never release physical goods to an unknown party who has made an EFT payment, nor make a refund without allowing time for the payment to clear first.

- **Devices with Vulnerable Firmware:** Many sites use devices, such as fibre routers, which are installed and left in place for many years. Over time vulnerabilities may be discovered in the firmware in these devices. The vulnerabilities are published and the manufacturers of the devices issue updated firmware to “patch” the vulnerabilities. However if the installed devices are not maintained and the firmware is not updated, they can be used as a vector to launch an attack on the site. We know of cases of “Mikrotik” devices being compromised in this way. Many devices are shipped by vendors with default passwords. Some devices, including hardware firewall devices, have been found to have hidden “back door” accounts, installed by the vendor, with pre-set passwords. In time these vendor passwords become known and published, which renders the device vulnerable until updated firmware is installed.

- **Compromised VOIP Account Credentials:** We have received reports of VOIP account credentials being compromised. The accounts were then used to make calls to international premium rate services. The account end users were held liable for the costs of the calls. Eventually the VOIP provider suspended services due to the client reaching their credit limit. Thus in addition to the financial loss end users suffered a disruption in services. VOIP devices should be secured and you should have appropriate credit limits in place with your VOIP provider.