CERTIFICATION EUROPE™

Organisation Details

Organisation Name (legal entity):	[314]
Sector:	[315]
Size of Organisation:	[316]
point of Contact Name:	[319]
Position:	[320]
Email Address:	[321]
Phone Number:	[322]
Address	[317]
Certifying Body (CB):	Certification Europe
CB Reference Number	[313]
Date of Application	May 30, 2017 at 11:01
Date of Last Update	May 30, 2017 at 11:01

Business Scope

[323]

CERTIFICATION EUROPE™

Boundary Firewalls and Internet Gateways

1.1 Give the details of any firewall or equivalent network devices
[329]
Comments
[487]
1.2 Who is responsible for the administration of the devices?
[333]
Comments
[488]
1.3 Who is responsible for setting usernames and passwords the devices?
[337]
Comments
[489]
1.4 Have the default passwords of the network firewall or alternative device been changed to use alternative and strong passwords or passphrases?
[341]
Comments
[490]
1.5 What approval process is in place for authorising network traffic to pass through the boundary devices?
[337]
Comments
[491]

1.6 Have unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), been disabled (blocked) at the boundary firewall or devices by default?
[349]
Comments
[492]
1.7 Do you have a corporate policy covering all firewall rules? If some rules are no longer required are they removed or disabled in a timely manner? Is this policy adhered to (meaning that there are currently no open ports or services that are not essential for the business)?
[353]
Comments
[493]
1.8 In what circumstances is the administrative interface used to manage boundary firewall configuration accessible from the internet?
[357]
Comments
[494]
1.9 Confirm that where there is no requirement for a system to have internet access, a default deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the internet
[361]
Comments
[495]

Secure Configuration

2.1 Have all unnecessary or default user accounts been deleted or disabled in all computers and network devices?
[365]
Comments
[498]
2.2 Do all accounts have passwords? Please confirm that any default passwords have been changed to strong passwords.
[369]
Comments
[499]
2.3 Have you ensured that any unnecessary software (including application, operating system utilities and network services) is removed or disabled?
[373]
Comments
[500]
2.4 Has the auto-run feature been disabled?
[377]
Comments
[501]
2.5 Has a personal/host based firewall (or equivalent) been enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default?
[382]
Comments

[502]
2.6 Is a standard build image used to configure new workstations? Does this image include the policies and controls and software required to protect the workstation? Is the image kept up to date with corporate policies?
[387]
Comments
[503]
2.7 Do you have a backup policy in place, and are backups conducted regularly?
[391]
Comments
[504]

User Access Management

3.1 Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals?>
[395]
Comments
[506]
3.2 Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?
[399]
Comments
[507]
3.3 Are accounts removed or disabled when they are no longer required?
[403]
Comments
[508]
3.4 Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals?
[407]
Comments
[509]
3.5 Are special access privileges documented and reviewed regularly (e.g. quarterly)?
[411]
Comments
[510]

3.6 Are all administrative accounts only permitted to perform administrator tasks, with no internet or external email permissions?
[415]
Comments
[511]
3.7 Do you have a password policy or process which requires or enforces changing administrator passwords (e.g. at least every 60 days) to a complex password?
[419]
Comments
[512]

Malware Protection

4.1 Has malware protection software been installed on all computers within scope?
[423]
Comments
[513]
4.2 How often does malware protection software have all of its updates applied, and is this applied rigorously?
[427]
Comments
[514]
4.3 Have all anti malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?
[431]
Comments
[515]
4.4 Has malware protection software been configured for on-access scanning, and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning?
[435]
Comments
[516]
4.5 Has the malware protection software been configured to run regular (at least daily) scans?
[439]
Comments

[517]
4.6 Apart from Anti-Virus Software, how are commonly accessed executables protected from being attacked by malicious files?
[443]
Comments
[518]
4.7 Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function?
[447]
Comments
[519]

Patch Management

5.1 Is there a mobile working policy in force that requires mobile devices ((including BYOD (Bring Your Own Device)) to be kept up to date with vendor updates and application patches?
[467]
Comments
[520]
5.2 Is out-of-date software (i.e. software that is no longer supported) removed from a computer or network device?
[463]
Comments
[521]
5.3 Are all application security patches applied within at least 14 days of release?
[459]
Comments
[522]
5.4 Are all operating system security patches applied within at least 14 days of release?
[455]
Comments
[523]
5.5 Is all software installed on computers and network devices in the scope licensed and supported?
[451]
Comments

[524]