Organisation Details

Organisation Name (legal entity):	General Impianti s.r.l
Sector:	Engineering services
Size of Organisation:	Medium (250 Employees)
point of Contact Name:	Paolo Moscatelli
Position:	Sales Manager
Email Address:	ict@loccioni.com
Phone Number:	003907318161
Address	via Collefreddo 8/9 Maiolati Spontini 60030 Ancona Italia
Certifying Body (CB):	Certification Europe
CB Reference Number	Paolo Moscatelli
Date of Application	March 12, 2019 at 15:59
Date of Last Update	March 12, 2019 at 15:59

Business Scope

Installation of industrial machinery and equipment
Technical testing and analysis
Other professional, scientific and technical activities n.e.c.
Manufacture of other general-purpose machinery n.e.c.
Repair of electronic and optical equipment
Electrical Installation.
Renting and leasing of other machinery, equipment and tangible goods n.e.c.
The scope will be our three plant situated in Italy within a radius of 10 km in the province of Ancona. Each plant has a Data Center, and they are connected together in Fiber. Two Data Centers are used in production environment (4 hosts, 1 fiber storage and 1 iSCSI storage each, for virtualization environment). This two Data Centers are configured for physical and logical Disaster Recovery and Business Continuity. 150 Virtual Machines are installed, running both Windows (70%) and Linux (30%) O.S. Email servers are installed and distributed in this two Data Centers.
The last Data Center is used for Backup Infrastructure.
There are 80 computers (Notebook and PCs) running both Windows 7 pro and Windows 10 pro, distributed in these plants and they are all directly connected to one Internet connection through the Firewall.
Internet connectivity is provided through a well known broadband provider. There are two firewalls configured in High Availability, supported by a contractor. No Cloud appliation are used. 65 Access point are controlled by a WLC.
Seperate networks are used for employees and guests. In total 60 VLANs and 2 DMZ are configured. 30 smartphone are used by the employees.

Boundary Firewalls and Internet Gateways

1.1 Give the details of any firewall or equivalent network devices

There are two Fortinet 600C firewalls that operate in high availability that control and aplly teh policies for the whole traffic among Internet connection, LAN and DMZ.
All incoming and outgoing traffic from firewalls is monitored and analyzed by a company that provides Cybersecurity service (with a probe).

Comments

1.2 Who is responsible for the administration of the devices?

Internal IT Department (system administrators)

Comments

1.3 Who is responsible for setting usernames and passwords the devices?

Internal IT Department (system administrators)

Comments

1.4 Have the default passwords of the network firewall or alternative device been changed to use alternative and strong passwords or passphrases?

yes, system administrators have dedicated accounts and passwords. The default password have been changed. 8 is the minimum number of characters in length, contains no more than two identical characters in a row and includes a mixture of numeric and alpha characters.

Comments

1.5 What approval process is in place for authorising network traffic to pass through the boundary devices?

Internal IT Department (system administrators)

Comments

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?

Services not used for business reasons are surely disabled by default. Other vulnerable services used for business reasons are enabled and constantly monitored.

Comments

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)?

Yes, the policies are reviewed every month. Only policies that are essential for the business are enabled.

Comments

1.8 In what circumstances is the administrative interface used to manage boundary firewall configuration accessible from the internet?

never. Only by LAN

Comments

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

The Internet access for the employee is granted by the LDAP authentication. Internet for guest is granted by a guest network that need a temporary user name and password provided on request (different for each user). Without these two type of authentication is not possible to navigate.

Comments

Secure Configuration

2.1 Have all unnecessary or default user accounts been deleted or disabled in all computers and network devices?

In each Computer only onedomain user is configured.
All domain users are periodically checked and disabled if no more necessary.

Comments

2.2 Do all accounts have passwords? Please confirm that any default passwords have been changed to strong passwords.

yes, I confirm. The password are set through complexity rules defined in the domain controller. 8 is the minimum number of characters in length, contains no more than two identical characters in a row and includes a mixture of numeric and alpha characters (at least one tiny and one upper)

Comments

2.3 Have you ensured that any unnecessary software (including application, operating system utilities and network services) is removed or disabled?

yes, predefined images are installed on the computers. Vulnerable or Dangerous software are blocked by the antivirus software. And the Cyber security probe check if a user install a dangerous software.

Comments

2.4 Has the auto-run feature been disabled?

yes it is enabled

Comments

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?

yes it is enabled

Comments

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?

The IT department create the images and is responsible to keep them up to date in terms of operating system and softwares.

Comments

2.7 Do you have a backup policy in place, and are backups conducted regularly?

yes, backups of servers are performed every night.
No backups regarding the computers (except for the emails).

Comments

User Access Management

3.1 Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals?>
yes the requests come from the manager or from the human resources department through a ticket request. The request is evaluated by the IT department to evaluate compliance with the security policies
Comments
3.2 Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?
yes through active directory services (LDAP). Each user has its own account (not shared) and the password is set through complexity rules defined in the domain controller. 8 is the minimum number of characters in length, contains no more than two identical characters in a row and includes a mixture of numeric and alpha characters (at least one tiny and one upper)
Comments
3.3 Are accounts removed or disabled when they are no longer required?
When no longer required user accounts and special access privileges are removed. When a user leaves (or for an individual changes role), the HR department communicate it to the IT department that disable or modify the account.
Comments
3.4 Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals?
yes through active directory groups. Admin account are only used by the IT department.
Comments
3.5 Are special access privileges documented and reviewed regularly (e.g. quarterly)?
They are not documented but they are reviewed periodically (every three month)

Comments

3.6 Are all administrative accounts only permitted to perform administrator tasks, with no internet or external email permissions?

yes. Domain administrator accounts are used only to make changes to the domain controllers.

Comments

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?

No, we don’t. Users are invited (by email) to change the password periodically.

Comments

Malware Protection

4.1 Has malware protection software been installed on all computers within scope?

yes, sophos endpoint security and control 10.8 version. Sometimes we use in addiction Malwarebytes and RogueKiller.

Comments

4.2 How often does malware protection software have all of its updates applied, and is this applied rigorously?

They are updated as soon as the supplier provides the update and automatically distributed through the centralized server.

Comments

4.3 Have all anti malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?

They are updated as soon as the supplier provides the update and automatically distributed through the centralized server, that show me the computers that are not up to date and give me the possibility to force the update.

Comments

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?

yes, the software it is configured through the centralized server for access scanning, including downloading, opening files, opening folders on external (USB) or remote storage units and scanning web pages. The user is not able to disable this configuration. We also have the Cyber security monitoring service for the traffic that help us in these issues.

Comments

4.5 Has the malware protection software been configured to run regular (at least daily) scans?

yes daily

Comments

4.6 Apart from Anti-Virus Software, how are commonly accessed executables protected from being attacked by malicious files?

control with the UAC and through the Cyber security monitoring service.

Comments

4.7 Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function?

through the firewall, the signatures and a dns defense service that blocks navigation to malicious ip addresses.

Comments

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?
yes, software updates are always activated and set to perform the installation automatically. If security patches for known vulnerabilities are made available, we are able, through an agent (OCS Inventory) or through the Group policy rules to install them
Comments
5.2 Is out-of-date software (i.e. software that is no longer supported) removed from a computer or network device?
Sometimes not applicable for software compatibility reasons. When possible we are able to do it through an agent (OCS Inventory) or through the Group policy rules
Comments
5.3 Are all application security patches applied within at least 14 days of release?
Sometimes not applicable for software compatibility reasons. When possible we are able to do it through an agent (OCS Inventory) or through the Group policy rules
Comments
5.4 Are all operating system security patches applied within at least 14 days of release?
If possible, for business reasons, yes we do.
Comments
5.5 Is all software installed on computers and network devices in the scope licensed and supported?
Regarding guests, they can only use the guest network. Regarding employee or supplier a written disclosure has been delivered personally to everyone. This disclosure explain the the correct use of IT devices (personal and business)

Comments