ETSI TR 103 305-3 V1.1.1 (2016-08)

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 3: Service Sector Implementations

Reference

DTR/CYBER-0012-3

Keywords

Cyber Security, Cyber-defence, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.3].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document is an evolving repository for guidelines on service sector Critical Security Control implementations. Because of their rapidly scaling importance and need for defensive measures, the mobile device and Internet of Things (IoT) sectors are treated.

Introduction

The individual service sector guideline clauses below provide subject matter introductions.

1 Scope

The present document is an evolving repository for guidelines on service sector Critical Security Control implementations. Because of their rapidly scaling importance and need for defensive measures, the mobile device and Internet of Things (IoT) sectors are treated. The CSC are a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks.

The present document is also technically equivalent and compatible with the 6.0 version of the "CIS Controls Mobile and IoT Companion Guides" October 2015, which can be found at the website https://www.cisecurity.org/critical-controls/ [i.1].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] The Center for Internet Cybersecurity: "CIS Controls Mobile and IoT Companion Guides" October 15, 2015.

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.2] NIST SP 800-101: "Guidelines on Mobile Device Forensics".

[i.3] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts that are maintained by the Council on Cybersecurity and found at the website https://www.cisecurity.org/critical-controls/

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
API	Application Programming Interface
ARM	Advanced RISC Machine
AV	Anti-Virus
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COOP	Continuity of Operations
CSC	Critical Security Control or Capability
DDOS	Distributed Denial of Service
DiS	Data-in-Storage
DoS	Denial of Service
EEPROM	Electrically Erasable Programmable Read-Only Memory
GSM	Global System for Mobile Communications
HART	Highway Addressable Remote Transducer
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion prevention system
IPsec	Internet Protocol security
IPv6	Internet Protocol version 6
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LE	Low Energy
MDM	Mobile Device Management
MSSP	Managed Security Service Provider
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OS	Operating System
OWASP	Open Web Application Security Project
PC	Personal Computer
PIN	Personal Identification Number
RF	Radio Frequency
RSU	Road Side Unit
RTOS	Real-time Operating System
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information Event Management
SP	Special Publication
SPAM	unsolicited or undesired electronic message(s)
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Secure Sockets Layer
TLS	Transport Layer Security
TV	Television
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

4 Critical Security Controls: Mobile Device Security

4.0 Introduction

Mobile devices are starting to replace laptops for regular business use. Organizations are building or porting their applications to mobile platforms, so users are increasingly accessing the same data with mobile as with their laptops. Also, organizations have increasingly implemented Bring Your Own Device (BYOD) policies to manage this trend.

However, many organizations have been struggling with the increase of personal mobile devices, and do not fully understand the security risks they may bring. There are concerns that their compact size makes them easy to lose, that they run newer operating systems that do not have decades of use and examination to uncover their weaknesses, and that there are millions of potentially malicious mobile applications that access data, spy on users, steal credentials, act as ransomware, or even become part of a Distributed Denial of Service (DDOS) botnet.

Like with traditional PC platforms, mobile still has to worry about protecting data from unauthorized access at rest and in transit; traditional network level man-in-the-middle attacks on public Wi-Fi; and similar web application threats (since mobile apps frequently access the same server endpoints as web applications). Employees today may use their mobile devices to perform the same business functions and access the same data as their PCs or laptops; but what is different is they are not physically connected to the corporate network, and likely, not even logged into the corporate domain. There are times when organizations use mobile VPNs to access the corporate network, but more and more frequently, mobile users access cloud services. It is not uncommon for corporate mobile users to access numerous cloud-based applications that reside outside their enterprise. Each of these has its own credentials, again rarely linked to enterprise. Getting visibility on the configuration, threats and behaviour of these mobile devices is a challenge, since there are no "eyes" on the device like those attached to the network.

But this environment does not preclude tracking the threats and risks. The Critical Security Controls for Effective Cyber Defense Version 6.0 (*Controls*) is that they are universal and high level enough to apply to any technology implementation. Everyone needs to start with: "What is the mobile device?", "What is the configuration?" and "What risks needs to be addressed?" Basically 1 - 3 of the *Controls*. Protection requires knowledge of what is being protected.

The real challenge to mobile security is the multitude of different mobile devices. With desktops, there are largely commodity hardware running less than half a dozen different operating systems, and through conscientious configuration management, usually a single or only a few different OS versions. Mobile devices have four different popular software platforms, with dozens of different hardware vendors, and dozens of different carriers that affect the platforms. The most prevalent platform presently has 11 OS version families, with sub-versions under them, which on most devices are non-upgradable or forward compatible, and exist on dozen of hardware platforms and carriers. So the permutations become enormous, and understanding the risks of each of these is overwhelming. This is why, for enterprises that have strict security requirements, it is best to issue standard devices.

Within the *Controls*, application security (CSC 6), wireless device control (CSC 7), and data loss prevention (CSC 17) all are relevant to mobile. Restricted use of administrative rights (CSC 12) is also something that could be implemented, some MDM and mobile security platforms, have the ability to restrict administrative privileges to end users, which will prevent removal of security protections or monitoring. Malware defenses (CSC 5) are very different than traditional PC platforms. Secure configurations can also be applied (CSC 10), insecure features and functionality can be limited (CSC 11), and cloud based boundary defense can be provided (CSC 13). All of these areas are described in more detail in the table below. Using the *Controls* can be the framework to develop a security method and process to manage an organization's mobile security risks.

4.1 CSC Mobile Device Security Description

Simple security steps should always be followed to reduce the likelihood from most Mobile threats: not Rooting or Jailbreaking a device; only obtain apps from the device vendor or the organization's app stores, not 3rd party stores; being wary of any app wanting to install a Profile on a mobile device, as well as if there is an "Untrusted App Developer" popup for the app; and not leaving a device unlocked for long periods of time. For each Control, table 1 details the control's applicability to mobile and specific challenges, and considerations for implementation of that control.

Table 1: Critical Security Controls (Version 6): Mobile Device Security

Critical Security Controls (Version 6): Mobile Device Security			
CSC #	**Control Name**	**Applicability to Mobile**	**Mobile Device Security Challenges and Considerations**
1	Inventory of Authorized and Unauthorized Devices	One needs to have knowledge of all devices used to access data and resources in the organization. Mobile devices are not perpetually attached to the corporate network like other IT systems, so new methods need to be used to maintain the inventory.	An organization cannot get an inventory of mobile devices by running a scan to discover what mobile devices are connected; companies can use email accounts, or active synchronization software to determine what mobile devices are used to access email (which is most popular application for mobile devices). Also, Mobile Device Management (MDM) can support this by installing agents on the mobile devices to push down configuration and security profiles, monitor devices for configuration changes, and provide access controls based on policy.
2	Inventory of Authorized and Unauthorized Software	There are millions of mobile apps across dozens of different platforms. Mobile apps can bring risks and threats to data and credentials. Being able to know what is installed, and control access to malicious apps, and insecure versions of apps is important to protect the organization.	MDM tools can inventory apps, and set policies and whitelisting to promote use of secure versions of apps. However there are privacy considerations in Bring Your Own Device (BYOD) scenarios, as the organization may not need to know what apps an individual has installed on their personal device for personal use.
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Like with PCs, secure configurations and monitoring of these configurations are critical to maintain trust with these devices.	MDMs can restrict access to cameras, white-list Wi-Fi networks, apply password policy enforcement, and inventory what apps are installed. Be aware, this last feature can be a privacy issue in a BYOD scenario. An organization may not want the liability of knowing or having access to employee's personal email, apps that track health information, financial data, personal contacts and calendars, apps used in their personal lifestyle, or their location. MDM tools can scale to hundreds of thousands of devices, and provide the necessary monitoring to be alerted when devices are out of compliance; for instance, if someone installs an unauthorized application, turns off encryption, or jailbreaks or roots their device.

Critical Security Controls (Version 6): Mobile Device Security			
CSC #	**Control Name**	**Applicability to Mobile**	**Mobile Device Security Challenges and Considerations**
4	Continuous Vulnerability Assessment and Remediation	Mobile vulnerabilities are usually linked to versions of the Operating system, or malicious apps. Because mobile devices are not always attached to the network, vulnerabilities cannot be identified and managed like as done on PCs, servers, or other permanently connected networked devices. Mobile vulnerabilities also can apply to many layers; hardware, OS (version), OS (configuration), individual application (of which there are potentially millions), network connection (cellular, Bluetooth, WiFi, NFC), app stores, physical location (i.e., countries where the government monitors mobile devices) and finally, whether the device is corporate-owned or personal (privacy requirements).	One cannot just run vulnerability scans on a network to scrutinize the mobile devices. Therefore, mobile vulnerability assessments should incorporate threat modelling, and understanding the devices, data, users, and their behaviours. MDMs can play a key role in gathering the information for the "what" and "who" for mobile management. Also, there are number of mobile security point solutions that address strong authentication, data and application security, security of data at rest and in transit, and protection from network based threats when connected to Wi-Fi, such as man-in-the-middle attacks. Organizations can choose to outsource management of their MDM platform and mobile support, similar to using Managed Security Service Providers (MSSPs) to monitor and manage network security devices.
5	Controlled Use of Administrative Privileges	Many intrusions use valid credentials obtained either through social engineering, or captured by other means. One important risk in mobile is protecting credentials stored on the device, because a user's email account could also be a system or Domain Admin account. Also, Admin control is different in mobile devices. Malicious apps are taking advantage of unfamiliarity with the mobile admin levels, and there are malicious apps that obtain admin rights so they can hide themselves from the user.	Mobile devices are part of the network based on their credentials, not based on their connection. It might not be possible to control admin rights on mobile devices, especially in a BYOD situation; but access based on least privilege may apply. It is dangerous to allow users to Root or JailBreak mobile devices, because it opens up risks to vulnerabilities running at that lowest level.

Critical Security Controls (Version 6): Mobile Device Security			
CSC #	**Control Name**	**Applicability to Mobile**	**Mobile Device Security Challenges and Considerations**
6	Maintenance, Monitoring & Analysis of Audit Logs	Monitoring is irrelevant if there is not a process to identify events and respond to them. And this response should be matched with the potential impact of the event. This is the human aspect: determining what events or alerts can potentially damage the organization, and execute response in a timely fashion based on that.	MDM and mobile security tools can provide visibility by having agents on phones that send events and alerts to a central server. These can be integrated with traditional Security Operations platforms. Different types of mobile monitoring sources can provide different data. MDMs use the more traditional network operations type of approach: Is the device live? What is the make model and version? Is it up to date? What applications are installed? Has the device been rooted or jailbroken? How much traffic is it sending and receiving? The security tools have more granular logging, such as installation of known bad or suspicious applications, application-level changes to data, network routing changes, SSL certificates used, VPN launching, and in the case of cloud filtering; traditional perimeter gateway logs for web traffic, or other application traffic. There is also the practice of monitoring account connections to the network domain or a specific application. Metrics should be actionable, not just "how many" of an event happened. More effective things to track are: Am I getting data from everything I should (how many devices are sending events)? Is the right data being collected (are all data logs the correct ones)? Another item to track is the turnover rate of mobile devices, which can be higher than laptops. Multiple user accounts may exist for the mobile devices.
7	Email and Web Browser Protections	Mobile devices change the traditional enterprise architecture by not only extending it outside a traditional perimeter, but also bypassing the need to route much or all traffic through the enterprise network due to use of cloud services. However, web and email threats are still a concern with mobile devices.	Traditional email gateway security controls for SPAM and phishing reduction, and malware and malicious URL links apply to mobile. Mobile security tools use an agent-based approach that gives a view to threats on and to the mobile device, such as malicious applications and profiles, and malicious WiFi networks or Man in the Middle web proxy attacks. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.