UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS
DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

MATERIA:
SEGURIDAD DE LA INFORMACION

MAESTRO:
FRANCO LOPEZ VELARDE, EMMANUEL

TITULO DE INVESTIGACIÓN:
ACTIVIDAD DE APRENDIZAJE NÚMERO 2: INGLES

FECHA ENTREGA:
LUNES 27 DE AGOSTO 2018

ALUMNO:
FELIPE DE JESUS RUIZ GARCIA

CODIGO:
214522077

CARRERA: INGENIERIA INFORMATICA (INNI)

SECCION: D02

CALIFICACIÓN Y OBSERVACIONES:

My essay

Security of information is precisely protect information; thetf alteration and make it available. But this will not be possible without Physical security, because it is the base of everything related of hardware, the mother of the information. Now, not exists devices that could support fire, or water or electricshock, Physical security is focus on take actions to avoid above accidents, but physical security cover more topics to ensure the correct integrity and healt of the hardware.

Today the dangers are to order at the least expected time. From a natural disaster to a vehicular accident.

Physical security includes site location preventions, users authorized to access to a servers, moderns ways to work (like working from home / great place to work), natural disaster, threads, criminals, sabotage, legal process, contracts with thirdparty services (such as internet provider …) , conflict of interest, loyalty divided, prevent attacks from inside, ex-employees angry) … can you see it, there is a lot of thing to keep in mind to ensure the availability of the information.

Meanwhile newtork threads are trying to grant access on a server to theft databases.. some unathorized person could use the server and take it very easily, jumping on the server without physically without problems: so, if the physical security is not very good, all every is vain (firewalls …) This is a problem regarded in the physiical acces with the “access control authorized”, the use of credentials, badge also the use of the advance human methods like the fingerprints.

The transnationals allow their employees very comfortable and flexible work forms, such as working from home.

However this also means a risk for the company, since the theft of a room in which a laptop, a small usb memory or even a cell phone is lost can lead to immersed business losses at catastrophic levels such as the loss of a patent…

Physical security also cover the protocols for critical situations, example, suppose you are the owner of a small startup with a lot of potential and a promising future with a very successful application, called uberG. Your company is very close to sell the app, but one ex worker is leaving the company… He is taking advantage of your company installations to provoke on electrical accident on the room server. Physical security should define what to do in these situations, where the main focus is the human lives.

Or in another scenario, the ex coworker is shooting to company doors, meanwhile is walking towards the room server, to take the data. The physical security defines standards to proceed legal, and avoid injures.

This include define guards to supervise the doors, ccvt cameras, supervise guards (seriously). Taking advantage of new smart technologies like the artificial intelligence, some alarms with sensors are very effective to control many situations, from a suspicious person or long storm.

My conclusion is that the Physical threads are always there, in front of us, in all their shapes, but we are making “something more important” until the situacion is critical, showsttoper...

In fact, the physical security involves more areas, costs and resources than you could think: from the site location until the housekeeping.

Why we wait until the critical pyshical situation to put attention or or the KPIs show all bad in the bussines… technical debt is growing and “then” could be fatal. In fact, time, time, time : is the key to be safeguard everything: “ better to prevent than cure” or “its better prevent than miss information” or “its better to prevent than lost your job”…

RELATED NOTICE

https://www.zdnet.com/article/hackers-can-infiltrate-police-body-cameras-to-tamper-with-evidence/

Hackers can infiltrate police body cameras to tamper with evidence *August 14, 2018*

The use of body cameras by law enforcement is a controversial subject. While such technologies can help protect police officers by deterring inappropriate physical behavior and also give citizens who have been unjustly accused of crimes some means of evidence to the contrary, the issue of transparency around such footage is still in question.
More security news

How to get VPN protection for your laptop while using a smartphone Wi-Fi hotspot
Elections 2018: Is misinformation killing democracy? The enemy is us
Want Google to track you less? Get an iPhone, ditch the Android
Windows 10 alert: All versions get new Intel patches for Spectre, Foreshadow bugs

A new, proposed policy, for example, will mandate that LAPD officers must release footage within 45 days, which will turn on its head current stipulations that footage is withheld unless critical to a court case.

Studies suggest that body cams have little effect on police abuse but footage may prove useful in criminal prosecutions, leading to the rapid adoption of such technologies.

Such technologies do not come without risk, however, and now it seems this potential evidence is now at risk of modification or outright deletion due to a multiple of vulnerabilities in body camera software.

Speaking at DefCon in Las Vegas, Josh Mitchell, Principal cybersecurity Consultant at Nuix outlined a variety of ways in which footage can be accessed remotely, potentially leading to the compromise of evidence.

As reported by Wired, Mitchell analyzed body camera models marketed specifically for law enforcement purposes by Axon's Vievu, Patrol Eyes, Fire Cam, Digital Ally, and CeeSc.

In all cases with the exception of Digital Ally, security flaws existed which permitted the researcher to cause havoc, including deleting footage outright, editing objects out of content, make changes to file structures, and re-uploading modified footage silently and covertly.

TechRepublic: Smartphone fingerprint sensor checks body temperature to boost biometric security

The security issues relating to these devices went deeper, as Mitchell also uncovered security problems associated with mobile apps, software, and cloud services that the body cameras connect with, as well as the widespread use of easy-to-guess and default credentials.

None of the devices tested uses cryptographic protections, and not a single video file was digitally signed.

If law enforcement agencies wish to use technology to gather evidence, the lack of signing is a serious issue.

Without being able to sign off the footage, video content cannot be validated properly or issued with timestamps -- which could call evidence into question.

Alternatively, threat actors could modify footage and there would be no way to detect this kind of tampering.

CNET: Armed police in London to wear head-mounted cameras

Police officers could also be put in danger due to another set of security issues. With the exception of the CeeSc model, all of the cameras tested have Wi-Fi radio capabilities and failed to properly mask the IP addresses linked to the equipment.

This means an attacker could track the location of the wearer, which is a serious security issue for the police, especially if they are in the middle of undercover operations. IP addresses could also be tracked for upticks in body camera activity which may suggest planned raids.

It may even be possible to install malware on the body cams, which would allow attackers to potentially crash devices, cause disruption, or even conduct surveillance of their own.

Mitchell deemed the security problems as "appalling," and told the publication that many of these devices are missing modern security protections and mitigations to prevent cyberattack.

MY NOTICE FEEDBACK

Keep in mind that the cameras are all places, in the street, in the shop, in a hospital, inside of the companies, inside of govêrnet.
If hackers are able to control cameras, kiddnaping and criminals could take advante of it, they could know where is storage or value that they want to take...