Linnaeus University
Department of Computer Science

Loco News – Program Security

Practical work #2, 1DV700, HT21

Loco News is a news magazine in a Swedish city. They print and sell their magazine on a weekly basis. The company has lately expanded from being a small local company to now have a national coverage with more resources available. The management and infrastructure have not kept up with the expansion and there are several areas where they need to improve to have a more secure and structured office. They also need to invest in some new IT systems and need help to make sure they will be secure.

Background

Loco News has 22 employees of which one person primarily works with IT management. They are now in the process of either hiring more staff to manage the IT systems or outsource part of operations. They do not have any resources to develop new software, and no one is really knowledgeable in IT Security.

Most of the work is done at the office, designing layout of the magazine, writing and the administration of the company. Most employees are working on laptops at the office. Since the company's reporters are now covering the entire country, it means a lot of travelling of staff is involved. At these trips, they usually bring one of the company's laptops.

The servers are located in its basement. The reason for the servers' placement is mainly that staff felt that the servers were making noise. They thought it would be more convenient to have them in the basement, taking advantage of the free cooling of the cellar that is offered naturally. The cellar space is not particularly large; it is shared with the neighboring company (a law firm). The law firm keep both their archives and some leftover furniture close to the space where Loco News keeps their servers.

General:

- There are 22 employees total
- Most of them have a laptop as their working computer
- 8 employees have a desktop computer as their working computer
- The people with the laptops are allowed to use them outside the work
- The employees' PCs have full admin privileges
- The operating system (OS) that are used by all the employees are mainly Windows 10, Windows 8 and Mac OSX Mavericks, Mac OS Sierra, but some also uses UNIX
- 1 person is the head of the office (CEO)
- 1 person is managing the IT equipment and also takes the role as chief technology officer (CTO)
- Each employee has to sign an agreement to a professional secrecy when being employed
- WiFi is accessible at the office
- Server room has no direct protection against physical access or accidents other than normal locks and a UPS for the servers
- Previously incidents: Hardware failures, Viruses and other nasty malwares: Denial of Service (DoS), Trojan
- Employees bring their own personal devices like smartphones and tablets
- On the servers they have many different repositories of information, previous editions of the magazine, image database, records of well-known people in society for future use in articles, financial and employee information about the company etc.

Equipment:

- 10 desktops (PC and Mac)
- 18 laptops (PC and Mac)
- 1 WiFi router using WPA (Wi-Fi Protected Access) with PSK (Pre-Shared Key)
- 4 WiFi repeaters to get better coverage
- 2 Dell Servers (VMware Windows Server 2012 & Windows Server 2016, One Ubuntu Server guest with 50 clients.
- 3 big newspaper printers/presses connected via network and 22 desktop printers connected via USB to each employee workspace
- Document & small data stored on non-encrypted free cloud-based service
- Important data stored on local server

Interview with the company's CEO (Goran)

Goran: Welcome to Loco News
Consultant: Thank you, we look forward working with you. What can we do for you?
Goran: We have expanded quite a lot lately. We also had some security incidents lately that tell us we need to improve our security. We have identified several things, but what we are most pressing now is making sure that a new system we are developing will be secure.
Consultant: Are you developing it in house?
Goran: No, we have hired some consultants for it, but we feel like we need to take control of some of the aspects of the development and especially around security.
Consultant: Tell me more about this new system.
Goran: It is an application to support our business processes.
Consultant: What more precisely will this new application help with?
Goran: We need to keep better track of where the information we use to write our articles comes from, the quality of different sources, volume, type of information, cost associated with getting it etc. The goal is to broaden our network of information sources but also use the existing one much better.
Consultant: So, if this works out, it could be an important system for the company.
Goran: Yes, we have high expectations of this system.
Consultant: It sounds like some information in this system might be sensitive and include private information about people. Did you discuss how to handle this sensitive data and if there are any laws or regulations you need to conform to?
Goran: No, we didn't get that far in the planning yet. That is one of the things we need help with.
Consultant: Did you decide where you would host this new application?
Goran: We have been thinking about either hosting it in our server room or on some cloud service. Again, we need advice on what would be best in our situation.
Consultant: Do you know anything about what processes the developers are using to make sure the application is secure?
Goran: They mentioned something about being ISO 27000 certified, but I don't really know what that means or how it will affect the security of the application.
Consultant: I see, what I can do right now is put a team of our security experts on this to evaluate any security related concerns with the application and give advice on things to consider during the development. We will give you a report that you can use internally but also in your contact with the developers.
Goran: Great! You are hired!
Consultant: How can we get more information about the company and the new application?
Goran: We have a small internal project group that works this; Dimitrios and Alexandra, you can contact them for further information.