Exam_2020

Oppgave 1.1

If I have to advice normal level users about security, my 10 tips would be:-

1. **We must keep our Personal Information Professional and limited,**
2. **We must keep our Privacy Settings On**.
3. **We must always Practice safe Browsing**.
4. **We must be sure that our Internet Connection is Secure.**
5. **We must be careful what we are Download,**
6. **We must make Strong passwords**
7. **Secure Site,**
8. **Be careful what you post on social media,**
9. **We must be careful to whom we are talking online,**
10. **The last advise is to keep our Antivirus program up to date ,**

#1.2

If I have to advice normal level users about security, my 10 tips would be:-

1. **We must keep our Personal Information Professional and limited,** we shouldn't trust anyone to whom we don't know. It will be good as much as we hide our private information.

2. **We must keep our Privacy Settings On**. because online marketers and hackers both love to know all about you. Both browsers and mobile operating systems have setting available to protect your online. For example, Facebook also have privacy-enhancing setting value. also, lifehacker.

3. **We must always Practice safe Browsing**; we know that hackers are always seeking for people who trying to connect with free wife. One attempt can be a dangerous for people to lose important data from their system and can be hacked with big loss. We also get malware which can be affected by you as well. Malware spread itself to whom you are connect in social media. Like Facebook, Gmail, Instagram.

4. **We must be sure that our Internet Connection is Secure** because hackers can hack our system from our router's IP address. If we found something wrong with IP adsress we must change the password of our router.

5. **We must be careful what we are Download,** cybercriminal's main goal is to send downloading malware. For example; app, programs, and some interesting video-link and popular game. We must not trust any add and link until we are known for it.

6. **We must make Strong passwords** because passwords are biggest weak spots in the world. Simply we used to keep our password as simple as regular. So, anyone can guess. Therefore, we must always have our Password Strong. For example; capital letter, number and any kind of symbol like.. Waz@229&itd#qsave. It should be at list 16 digit.

7. **Secure Site,** we must use Online Purchases From Secure Site because, when we purchased anything we have to used our credit card or bank information. What exactly cybercriminals looking for.

8. **Be careful what you post on social media,** because once we posted on the social media they can copy and used even you deleted from the Site. Basically hackers do used you profile picture to misused or open you profile.

9. **We must be careful to whom we are talking online,** they can not be real always. They can be used fake profile and manipulating the people to get something what they want from them.

10. **The last advise is to keep our Antivirus program up to date ,** yes Internet security software cannot protect every security threats, but it will always detect and remove most malware. We must make sure that we keep update our operating system.

 # 1.3

1. Before employees can start using the internal systems (websites for managing information, OS applications, email clients, etc.), they will need to have been introduced to the systems with a focus on safe use and "cyber security" by the IT/security department, to ensure the employee follows some guidelines on what is safe to do, and what not to do with these systems.
2. If the company has a VPN, this should always be turned on when doing work related things, and/or when using the work laptop.
3. Do not mix personal and work documents, accounts, software etc. Ideally there should be one computer / OS for work, and another for personal use.
4. Do not use or engage in other software or services that has not been whitelisted by the company, including cloud storage, websites for converting documents to other filetypes, etc., etc.
5. Only use permitted software/channels for communication of work related things. Avoid using personal accounts/software/services during work time and/or at work place.
6. Do not try to fix technical/IT problems on your own, go to the IT department and have them help you.
7. Be aware of how a malicious person/party might try to achieve by targeting the company, so the employee understands the risks and what to look out for.
8. Clear guidelines on how passwords are managed and stored/saved.
9. Do not leave devices unattended / signed in.
10. Always think before opening any link or attachment in emails. If unsure or suspicious, ask the IT department to be safe.

 # 1.4

From the Oppgave1.1 and 1.3 both trying to advise that, if they hacked for example the whole company can be destroyed. Yes it is nice that our technology is developing every day, but at the same

time cybercrime also increasing day by day. We do not have completely solution to solve the cybercrime, but we personally can be aware and can make everyone aware by providing the prevent trending from cyberattack from IT specialist/department.

Oppgave 2.1

All digital devices in the kindergarten run on the same wireless network.

which is the worst-case scenario when only connecting to a network gives the attacker a flood of information about each and everything of children and parents

The employee uses their mobile phone for everyday work instead of the systems provided by KG.
The mobile phone is connected to the leading network where servers, cameras, and IT web portals lie.

> Mobile may have an older version of Firmware, may contain malware app which may intercept in the network and execute a remote attack and access all live footage of students and access all related documents which are a significant threat to the security of a student)
The printer is on the same network, which has access to many employees and Parents. It may be connected to other non-official person's devices.

If someone bulk printed the documents intentionally or mistakenly, then KG may suffer loss and scanned copies of students can be accessed through it, which is alarming for child safety.

The KG runs a web-based IT system, and a (Third-party) Consultant developed the whole system in 2013, which no longer provides Maintenance to the system.

This system stores photos, names, birth number, allergies, religion, family situation (such as siblings, signs of parents, persons who are allowed to pick up the child, etc.), illnesses, contact information for parents, pedagogical/physiological observations of the child and reports of concern to the child welfare service. In addition, information about delivery/pick-up/illness/absence is stored for the children every day.

Third-party development is always risky, and without Maintenance, it is vulnerable. When connected to a shared network, storing all information in one place is very risky. Intruders can access all information in one place, which is worse. And The data from the IT system is physically stored on the desktop office machine controls, where also the server part of this system runs. System and Data are saved physically in one place and one room which is absurd. Intruders only need physically available data without a plan; how easy would it be?
And Backup is only taken once per day, which is not good practice.
It needs to be synced in real-time, so nothing misses from the data.

All employees in each department have the same username/password of the system so that you log in as "department" and not the person.
We don't know who acted so that the wrongdoer will escape, and we only see the system log as the Department name, which is an easy escape for the wrongdoer.

An ordinary employee can enter and update the student data about disease, pick-up/sick etc., which leads to irresponsible data entry and

unknown employees, which may invite to a severe accident (allergic food and wrong time of pick-up may lead to misinformation in the time of investigation if something goes wrong)

The parent's portal is also connected to the same system, and the password is given unencrypted to the parents. Which is if missed then would be a big problem.
Also, hackers may execute the remote attack from the parent's side, which is connected to a central only server, a severe threat to student safety.

#2.2

The server and Web-Based IT System are connected to the same Shared Network.

- All Digital systems in the KG are connected to the same shared network, which poses a significant threat to students' safety. In addition, hackers can also access it easily as they do not need to penetrate network firewalls.
- Hackers can blackmail parents as they know all the parents' financial status and execute kidnap as they can interfere with cameras in the same network and place their name as pick-up guardian.

All employees can log in as a department but not as Individual and Shared Passwords.

- If the ordinary employee (not in charge of any responsibilities) can perform all operations without getting a catch. It also motivates an easy platform to perform any wrong act related to child safety.
- They can place wrong information on outsiders and leak the data, which will pose a threat to child safety.

Not maintained and old system developed by Third Party.

- Old firmware and old security are already vulnerable, which can be bypassed using many techniques. The security firewall is a decade

older, which is never pathed. This kind of system gives easy access to the hackers without noting logs and any alarms.
- The third-party may have their codes inside Software that bypasses all data to their system. So leaking information is a very happing incident by third party companies.
- Not maintained/updated/not patched system is far worse than a non-protected system with a regularly updated system.

#2.3 Oppgave 2.3 – 12,5 %
Diskuter hva innføringen av GDPR kan bety for barnehagen. Både konkret på mangler og tiltak som bør gjøres, men også mer generelt på sikkerhetsarbeid og
prioriteringer.

Data protection is in the school is most important. to protect information of the student and the employee. Also, it is important to hide the policy of the school. In the school there will be very different data like addresses, medical information, image, and more. Additionally, information related to job applicants, governors, staff and volunteers is often stored within a school database.

In this case, kindergarten should not access the same wife. They should use the network differently for guest and for the local use. Password should be strong, and they should take care when working remotely. Let all the employee and student know general knowledge about not to open any link and email which is not related to. They should not forget to install the anti-virus and malware protection. Basically, in the school or office any company they shouldn't leave the paperwork on the table or laptops unattended. Make sure your Wi-Fi is secure. Make sure that devices are not using without permission by parents/student of the kindergarten. Also we can place the encrypted system in kindergarten. So, it will not be worse rather than non encrypting system.

Oppgave_3

What is CSRF attack and what is the solution?

A typical Cross-Site Request Forgery (CSRF or XSRF) attack aims to perform an operation on a web application on behalf of a user without their consent. In general, it does not steal the user's identity directly, but it exploits the user to perform an action without their will. the attacker causes the victim user to perform an act unintentionally. This could be, for example, changing e-mail address on your account, change your password or make an unauthorized money transfer. To avoid the CSRF token is The most popular method to prevent counterfeiting of cross-site requests is to use a challenge token associated with a specific user, which is sent as a hidden value in all state change forms in the web app. And we have to be careful about what we are Download and log out after using the pages.

Exam_2021

Oppgave_1.1

a. **Hvilke sikkerhetsutfordringer byr dette på?**

   Due to working from home increased cyber security risks. We were far more vulnerable to cyber attacks without the security protections that office system affords us. Such as firewalls and blacklisted IP addresses, GDRP and remote working. GDRP mean is a security for own employee by the company. But when it became working from home, then it became out of control to handled it. As I realized the list of challenging are here: -

1. **Open home Wi-Fi networks: -**
   Normally everyone uses home Wi-Fi. So, it led to leaked data or hacked**.**
2. **Phishing Emails: -**
   Almost every employee had faced difficulties to identifying a phishing email due to lack of cyber-security awareness.
3. **Weak password system: -**

Even if your company makes use of VPNs, firewalls and security software, your business may still be at risk from employees using weak passwords on their accounts. Because they could guess easily, or it can be used by forced.

4. **Unsecured Home Devices: -**
   When everyone began working from home when the pandemic hit, some of your employees may have started using their personal devices for work. Whether it be mobile phones in place of a work telephone, printers, tablets or laptops, one of the main risks this raises is the lack of IT security infrastructure. Whether people are using mobiles to log into business accounts, taking sensitive calls from clients or may have voicemails in their inbox which contain important data, many employees will not think to ensure these are encrypted.

5. **Unencrypted File Sharing: -**

While companies may think to encrypt files saved on their network, they might not consider file encryption when data is sent from one location to another. From client account information to customer data, and financial information, your company cannot afford for cybercriminals to intercept files when they are being shared. When files are stolen in this way, it can lead to identity theft, ransomware and theft.

#B.

While employee working from home, they must follow the company's guideline. And if you are working from outside of your office protection system, be sure that you have secure connection. VPN (Virtual Private Network) service is the best methods to protect the traffic from your computer. It will be the best if you always try to use company devices for work related tasks. Because your device equipped with best protection that are quality-assure by you IT

department. While employee have to share the document or file, they should always use cloud services approved by company. Also, employee should always sure that work device should not use by others. Be aware from fishing attacks. Be sure what link and app are you downloading. Is it a http or https you always make sure before open it. Is you have sensitive information then don't share by email? You can choose cloud service instead of by approved your company. If you found something wrong, then always contact IT department instead of trying to solve by yourself. Taking back up after the everyday work.

#C. Hvilke mulige tiltak og rutiner kan bedriftene innføre?

To give approval for employee to work from home is the best solution on corona pandemic, but without any security concern. The companies seem irresponsible for the security purpose. So, the company should collaborate with IT department about the strong security. From the company side should think about these lists of security: -

- Communicating remote-work security policies setting,
- VPNs (virtual private network setting),
- Regulating personal-device use.
- Addressing authorization and authentication.
- Give the training for employee about phishing and malware, malicious to the current crisis before they start work from home.
- Company can secure the methods of communicating channels. Like zoom. Team, skype etc.
- Proving vigilant IT support.
- Teaching employee to take back up every day after work.

The company need to analyze about the secure guideline information security.

Oppgave_2

a. **Hvilke sikkerhetsutfordringer/risiko kan dette medføre (enkelte punkter vil variere noe fra enhet til enhet, så få med forutsetninger for de litt mer spesifikke risikoene, slik som "har kamera")?**

- ⇨ Data collected from your robot vac can be used in a lot of different ways. A map of your home can be important information for a hacker that plans on Robbing you or collect the compromise video of you from the robot vac's camera and starts threat you. A hacker can gain access to your robot vacuum's app through malware on your phone and gather information or control the bot. the manufacture also collects the information and can share or sell it to advertisers or start blackmail and start asking money for it and they will be not done with once or certain amount of money. They will continuously be asking you a bug of money.

b. Hvilke mulige tiltak man kan gjøre?

- ⇨ After they lunched the robot vac many people attracted to use it. Yes, it is useful to use it. Who doesn't have to be at the home but you have to clean the home, The app made it easy? They can use it by the phone directly through app. Later on many people have faced the difficulties by hacking through this app/camera. There are few things that can prevent your data from being hacked. Which are:-

1. Use you vacuum offline. It means using the vacuum with just its remote control or the onboard buttons and not the app. This way, the robot is not connected to the Internet, and information can not be accessed. Yes, there is more useful features of your vacuum, like scheduling a cleaning, won't be available anymore.

2. Another way is factory reset. So, disconnect your vacuum from Wi-Fi completely to disconnect a Roomba you're your internet. There are many ways to do it. Make sure vacuum become reset completely.

3. You can update vacuum software regularly to remove any bugs that may be exploited by hacker to gain access. It won't prevent the manufacturer from gathering data, but at least it will stop hackers. Be sure that you are updating you vacuum regularly.

Oppgave 3

The banking sector always has been under danger to be hacked. Intentionally unintentionally bank is in always main place to be hacked.

Today it's not only cyber fraud but hacks into servers to obtain a customer's personally identifiable information (PII). That is why cyber security is very important for banking. In banking sector perform most transactions online by individuals and company. cyber security is that system which can encompasses everything that relates to protecting our data from cyber attackers who want to steal or theft our information and use it to cause harm.

I'm wring a story that I have shown A few years ago, a bank hacked by hackers. The bank lost all the data information's. and, they didn't take the back up after the day every day for 1 weeks. The reason is as I heard that there was a problem with backup system. After this hacking they had to pay a lot of money to release that data. After that incident many of customers closed their account from that bank. Because bank lose the trust of customers. That is why I strongly recommend you analyses about the cyber security and implement all the prevent protection from cyber attacker.

I have made a list why cybersecurity is important? Here some are: -

1. To protect customer's data information and assets we need the cyber security. As many people choose for cashless and activities are done through online checkout pages and physical credit scanners. In this case PII can be redirected to other locations and used for malicious activities. It also greatly harms the bank while they attempt to recover the data. If they hacked the bank need to pay unlimited money to release the information. They will lose the trust of their customers and other financial institutions.
2. More attack in the mobile app. On mobile app individually access their bank accounts. This makes the potential of attack much greater. Therefore, banking software solutions are required solution to prevent malicious activity.
3. When bank upgraded their cyber security, hackers share banking systems and third-party networks to gain access. If these aren't as protected as the bank, the attackers can get through with ease.
4. There is a risk for cryptocurrency in this world. The sector is unsure how to implement cyber security software for banking changing market. And this sector turned for the hackers at easy to hack and it quickly changed in a value.

Yes, there are many problems with security and this problem is cannot ride off fully. So here are some security's tips for World of banking software development to secure the organizations.

1. Security analysis is imperative before any new cyber security software is implemented. It will provide recommendations that can help save money while also allowing for proper investments.
2. Cyber security banking configuration must choose right hardware to block attacks including applications. With an updated firewall, banks can block malicious activity before they reach other parts of the network.
3. While a firewall upgrade increases protection, but it won't stop attacks unless anti-virus and anti-malware applications are updated. You have to regularly update the anti-virus to make sure it works.
4. There is extremely critical to protect customers who utilize mobile or online apps to do their banking. In this case we can choose the multi-factor authentication to approve the app/sever open. The best thins to apply MFA to stops attackers from reaching the network because it asks for another level of protection. For instance, a six-digit code sent to a customer's cell phone.
5. Also, we can make our system automatic logout. Many websites and app allow a user to stay logged in if they allow it. Hackers can get information anyway but, these methods will not let hackers easily to get access the information.
6. For any employee who are working or who are going to work it is important to trend or give the class about cybersecurity by IT department.
   This all what I can say why bank need cybersecurity in the organizations.