UNIVERSITETET I AGDER

KANDIDAT

8416

PRØVE

IS-214 1 Informasjonssystemsikkerhet

Emnekode	IS-214
Vurderingsform	Skriftlig eksamen
Starttid	28.11.2017 08:00
Sluttid	28.11.2017 12:00
Sensurfrist	19.12.2017 00:00
PDF opprettet	17.11.2019 12:47

Oppgave	Tittel	Oppgavetype
☑	IS-214, general information	Skjema
1	IS-214, question 1	Langsvar
2	IS-214, question 2	Langsvar
3	IS-214, question 3	Langsvar
4	IS-214, question 4	Langsvar
5	IS-214, question 5	Langsvar

☑

IS-214, general information

Course code: IS-214
Course name: Information Systems Security

Date: November 28th
Duration: Four hours

Resources allowed: Dictionary

Notes: Attempt all the questions.

The professors sometimes ask for exam answers to be used for teaching purposes, but in order for this to take place, the university needs your consent.
Do you grant the University of Agder permision such permission?
Select one alternative

- (•) Yes
- ( ) No

1

IS-214, question 1

What is CIA model? Explain with an example of online shopping site.
(Marks: 10, answer should be around 200-300 words)

Fill in your answer here

The CIA modell is an acronym describing a model used to ensure the confidentiallity, integrity and availiability.

This will help to ensure that when setup a company or a site that you'll be able to keep the information confidential to people that shouldn't have access to it. Meaning you wouldn't give people access to read your database filled with user credentials, this breaks the confidentiality "rule". also the triangle won't be complete without confidenitality as this is a really big deal of the CIA model.

Integrity, is to help ensure that the data on the site, like anything that is in stock, is in stock.. that it can be trusted with ones credit card and personal information.

Aviliability will help to ensure that the hardware the online shopping site is used on is always working properly. So this will say that you will always maintain the hardware and ensure it's at peak performance, if a problem was to occur, you would have to repair these problems as quickly as they apeear.

Confidentiality

This part is where you'll ensure who has access to what.

Integrity

Consistency, Assurance and Trustworthiness of it's data and to maintain that its what it is.

Avaliability

Maintaining hardware, reparing hardware problems when they occur.

2 # IS-214, question 2

What is the difference between symmetric and asymmetric encryption systems? Give some examples.
(Marks: 10, answer should be around 200-300 words)

Fill in your answer here

Symmetric encryption is method of encrypting and decrypting data with only one key(The same one). This means that it's one key to decrypt the message and the same key to use for encrypting the message.

This way of encrypting a message is highly unsecure. An example of an symmetric encryption is ROT13, which is a rotating chipher where you'll shift each letter in the message 13 places, before doing it to the next letter. There's a joke with this saying " We wanted our message to be secure so we encrypted it not only once but twice with the ROT13.." this meaning it's message isn't as secure anymore as it should be, by applying the ROT "encryption" twice gived one the same message in clear text, as it's shifts the character 26places.

Asymmertic encryption is like the symmetric encryption but instead of having one key, it's being used to two keys. one Public key and a Private key, this makes it really secure. The public key is used to decrypt the message and the private key is used to Encrypt the message. So if Alice and Bob was to send a message. Alice would give Bob her public key and vice versa with bob. So since now both bob and Alice have the counterparts public key, they are now able to send encrypted messages to each other. So if someone was to intercept and find the message it would appear as jibberish, since it would not be readable without the senders public key. This method of encrypting messages is really being used to day, it's Called RSA. And can be used when making an ssh-connection to a server. These public keys and private keys are built up using large combinations of prime numbers making it really hard to bruteforce.

3 IS-214, question 3

If you have to do the risk assessment of a banking organization then explain the process that you will follow.
(Marks: 10, answer should be around 200-300 words)

Fill in your answer here

risk assesment is a process of ensuring the safety of the target one is going to do the risk assesment of. So if i was to do it of a bank. I would proceed by locating the services of the bank, what is it running, how does it handle the information it's given, how everything is handled, is it handled securly, aswell as the physical security. One would have to go over all the weakness of the banking organization.. and see what could make an risk on the banking and start evaluating on the banking organization, what impact will this make.. what harm will this cause the banking organization..
aswell how much will one loose depending on the servers.. how much is it worth.. how much does it cost to have it running each minute, and for each minute of downtime how much would one loose... and so on.
You would have to calculate each of the services how much would one loose on each service was it to go down and make it impossible to access the bank's services..

4 IS-214, question 4

Explain four types of security culture with an example of a university.
(Marks: 10, answer should be around 200-300 words)

Fill in your answer here

Clan

- This is a flexible culture where as people stay for longer periods of the time.
  - Can be found in non-profit organizations

Adhocry

...

Market

...

Hiarchery

- This is a more strict security culture stating that the people at the top would be in charge and people at the bottom would be at the lowest ranking, one would find this kind of culture in military and government situations. where there's a set of ranks and such configured for each step...
  - Widely used in military settings, and govnerment.

5 IS-214, question 5

Read the Case Description carefully and answer the following questions.
(Total marks : 60, each question carries 12 marks)

1. There is a point about required length and compositions of passwords: What is your opinion about being forced by the system to create complex passwords?

2. What do you think about the virtual dollars used in the case? Is this a secure way of paying at the university campus?

3. The case shows that the system security isn't good enough and is lacking a security policy. What would be the most important points for the University to add to such a policy?

4. The Transaction Management System (TMS) had changed hands multiple times within the last ten years. To ensure better competence and security around the system, would it be better to let only one division have the full responsibility of the system, instead of splitting the system responsibilities among the different divisions?

5. What is your impression about the security culture of this university?

Fill in your answer here

1. **There is a point about required length and compositions of passwords: What is your opinion about being forced by the system to create complex passwords?**

   This case had no such thing to create a complex password, here in the case password could be as small as 3chars, no special characters, it could be used throught it's study period without having to change it once.

   By being forced to change the password every so 90 days is a bit of a hassle, for the point being either you have to be creative or you have to generate a 24 chars long string conatining many special characters. It's needed, to argue against having to change the passwords is a lost cause. It's what you have to do to keep a clean and secure system. It's like a toothbursh, at some point it's brushing hairs will be old and not as good as it once was. This can bee seen as the same with password, first it's long, secure.. and when some time passes you are in need of changing it since it's old and outdated, and you want to keep it secure.

2. **What do you think about the virtual dollars used in the case? Is this a secure way of paying at the university**

campus?

The so called "virtual dollars" sounds like the cryptocurrency bitcoins, however the virtual dollars used here in this case seems like a fast and easy way of getting what you need when you want. In the case it does not say how one pays with the dollars, so I would make a conclusion and say it's being payed with cards that has RFID/NFC support making it pay with a simple touch of the card on a bank terminal. However, this feels a bit to much. To be able to pay for a plan where you'll go buy whatever you want whenever you want, is not far from how one would go if it was on a university as UiA with regular dollars and credit cards. Virtual dollars is self explanatory, it's all in the cloud so to speak, this makes the counting of todays income really simple as it's no more of double checking with the cash in the register aswell as checking what the machine says, as so to see how much was in the machine when you started at work...it's truly a hassle. With virtual dollars this is really handy, but then it's all about the security of the virtual dollars.. where is the information being held about the transactions...I think that personally it would be quite intressting to switch out "physical dollar" with virtual dollars, it feels like one is in the future but in perspective it's more or less the same as said earlier to just pay with "physical dollars" than with "virtual dollars"... It feels as secure as it is unsecure, meaning it's just as unsecure as any other kind of paying.. thou here the "virtual dollars" had to be used in the university's shops.. and it would be a prepaid amount on the card.. rather than a credit card you would in a way have a "prepaid amount" on the card meaning you could spend as much as the card had on it's balance.. all in all it's secure until the point someone's tries to hack this system. The ABC university had the Virtual dollars on a server with a simple frontend and backend containg a database. This purposes as a higly security threat, and should be rather more secured than one server..

3. **The case shows that the system security isn't good enough**

and is lacking a security policy. What would be the most important points for the University to add to such a policy?

They would be in the need of creating good policies regarding making good and secure passwords aswell as making it clear to anyone that is employeed at the ABC university that sharing password with others is not acceptable, either it's over phone, email or with Post-it®. The password is like a toothbrush you wouldn't share it with others, othen than yourself. Regarding complexity of the password, you would have a set of requirements stating that it needs to be
* atleast 6 chars long,
* need to contain one upper case letter
* a number
* and a special character.

To ensure that each password is secure.

4. **The Transaction Management System (TMS) had changed hands multiple times within the last ten years. To ensure better competence and security around the system, would it be better to let only one division have the full responsibility of the system, instead of splitting the system responsibilities among the different divisions?**

By both splitting and not-splitting is both good ideas, but thou are not good ways of doing things, if the routines are not good enough.. one of the best ways of doing things is to give the rigth departement the rigth access. This will take some time to tailor it so that each department gets access to what they need access to. Meaning that Financial departmen shouldn't have access to the system meaning that they shouldn't be able to export out all of it's data. One would make an analysis of the system, and then decide in a good manner with focus on security who should get access to what, and should they be able to have read and/or write access to the specific data. So this would give the Finanicial department access to read certaint things

from the user database like, firstname and sure name, what meal plan do they have and if they have payed for their plan, aswell as keeping track of their balance to see that they aren't tricking the system into getting things for free. They would have access to run the diffrent buisness intelegence reports.

To change out the employees does ensure that you get younge folks with more updated experience. But TMS should have implemented better hiring routines regarding learning up new people to handle the system. When hiring new employeers, there should a routine where as the new employee should go through 2-3weeks learning period with pay depending on the size of the system he's given administator prviileges for. So that if trouble was to happen newly employeed workers would know what to do.

5. **What is your impression about the security culture of this university?**

By the state the university is in it's a fairly poor one.. i would say adhocrhy