REFLECTION REPORT

RIHAM AHAMED ABDUL RAHEEM
HND COMPUTING IDM

UniCare being an insurance expert and being vastly related to money must align with the best security software available. In the policy, I have described and proposed the usage of a several systems such as using virus guards, cameras, access hierarchies etc.

In this reflection I will recommend specific software and I will then give a brief personal opinion on how UniCare's security can be bolstered by using said software.

Antimalware & virus guard:

MalwareBytes - They provide team based subscription plans and cover everything from email protection, and grants the user a highly lethal force to combat modern day threats. They have several other minor software to combat adware and rootkits also.

Encryption algorithm:

Advanced Encryption Standard 256-bit in GCM mode, this algorithm is strong enough to keep sensitive information safe. It is directly endorsed by Microsoft (used to encrypt wifi passwords etc).

Hashing algorithm:

Secure Hash Algorithm 256-bit, as per the policy hashing before encrypting and dissolving the hashing after decryption of all passwords.

Packet-sniffer:

Wireshark or Metasploit, both software can be used to sniff packets and monitor the network but metasploit is more based on exploiting, still metasploit can be used to identify the loopholes in the security of the network.

Vulnerability scanner:

Nessus, highly used in the industry to identify vulnerabilities in systems, during auditing and the precedence after an incident it is highly recommended to use such a software.

The standards I have described in the policy must be thoroughly practiced without exclusion however the management panel has full authority to overcome these declarations through majority vote.

The policy I have put revolves around countering modern day threats that have occurred frequently throughout the world, UniCare must make sure that employees are trained.

The above mentioned tools must be used in order to streamline security without cutting into the budget the company has. The reason why there is as less possible security tools used in the policy and mentioned here is that, without doubt every tool comes with its own problems and sometimes vulnerabilities in order to minimize this risk and to maximize security to highest level possible.

I decided to take this decision after a several tech giants took a huge hit in the past few months, and it was later revealed that it a significant percentage of the reason why they became vulnerable was due to the vast stack of security applications they used.

I have backed my decisions with reason, facts, knowledge and personal opinion as such my policy will not be the best for all but it definitely will be the best for what it's targeted for.