NOSLĒPUMU UN PAROĻU GLABĀŠANA UZŅĒMUMA VIDĒ

Autors: Andris Pakulis
Darba vadītājs: Dr.dat. Krišs Rauhvargers

KURSA DARBS

Problēma

Problēma → Pētījums → Rezultāts

Informācijas laikmetā ir vienlīdz svarīga informācijas drošība un pieejamība. Katrā uzņēmumā ir nepieciešamība pēc noslēpumu glabāšanas veida, kas samazina to izpaušanas un pazaudēšanas risku, ņemot vērā daudzus faktorus – ārējo apdraudējumu, nelojālus darbiniekus, darbinieku mainību.

- Šifrēta rezerves kopija, kuras šifra atslēga pazudusi
- 2006.gadā izveidota SQL konta parole,
  kas pēkšņi nepieciešama, bet neviens to neatceras
- Servisa lietotāja parole, kuras izveidotājs vairs nestrādā uzņēmumā

Mērķis

Apzināt mūsdienās aktuālos kriptogrāfiskos algoritmus, to nepieciešamos atslēgu garumus, kā arī apzināt aktuālās kriptogrāfiskās shēmas, to pielietojumus un novērtēt to iespējamo pielietojumu, kā arī izveidot dažus risinājumus noslēpumu glabāšanai uzņēmuma vidē.

Turpmākais darbs

Maģistra darbā plānots aplūkot dažādus noslēpumu glabāšanas gatavos risinājumus, kā arī, balstoties uz iegūto informāciju par kriptogrāfiskajām shēmām, izveidot metodiku noslēpumu un paroļu glabāšanas risinājumu izvēlei atkarībā no prasībām un iespējām, ņemot vērā pasaules labākās prakses un drošības aģentūru vadlīnijas.

Teorētiskās daļas izpētes rezultāti

- Izpētīti modernās kriptogrāfijas algoritmi un to drošības līmeņi
- Izpētīti un apkopoti populārākie kriptogrāfijas pielietojumi un to shēmas
- Identificētas vēlmes specifiskā vidē nosacītam uzņēmumam
- Izveidots potenciāls risinājums/shēma noslēpumu glabāšanai uzņēmuma vidē, ņemot vērā potenciālos apdraudējumus un riskus

Nedroši (novecojuši)	Legacy (derīgs esošām sistēmām)	Derīgs nākotnei
MD5, RIPEMD-128	SHA1(160), SHA2(224), SHA3(224)	SHA2(256/384/512) SHA3(256/384/512), Whirlpool(512)
DES	3DES(128), Blowfish(160)	AES(256+), Camellia
RSA(<1024), ECDLP(<160)	RSA(1024+), ECDLP(160+)	RSA(3072+), ECDLP(256+)

Ieteikumi drošai kriptogrāfijai 2016.gadā un nākotnei
NIST (*National Institute of Standards and Technology, ASV)* un ENISA (*European Union Agency for Network and Information Security*)