Chapter 3

Information Security and Risk Management

Company
LOGO

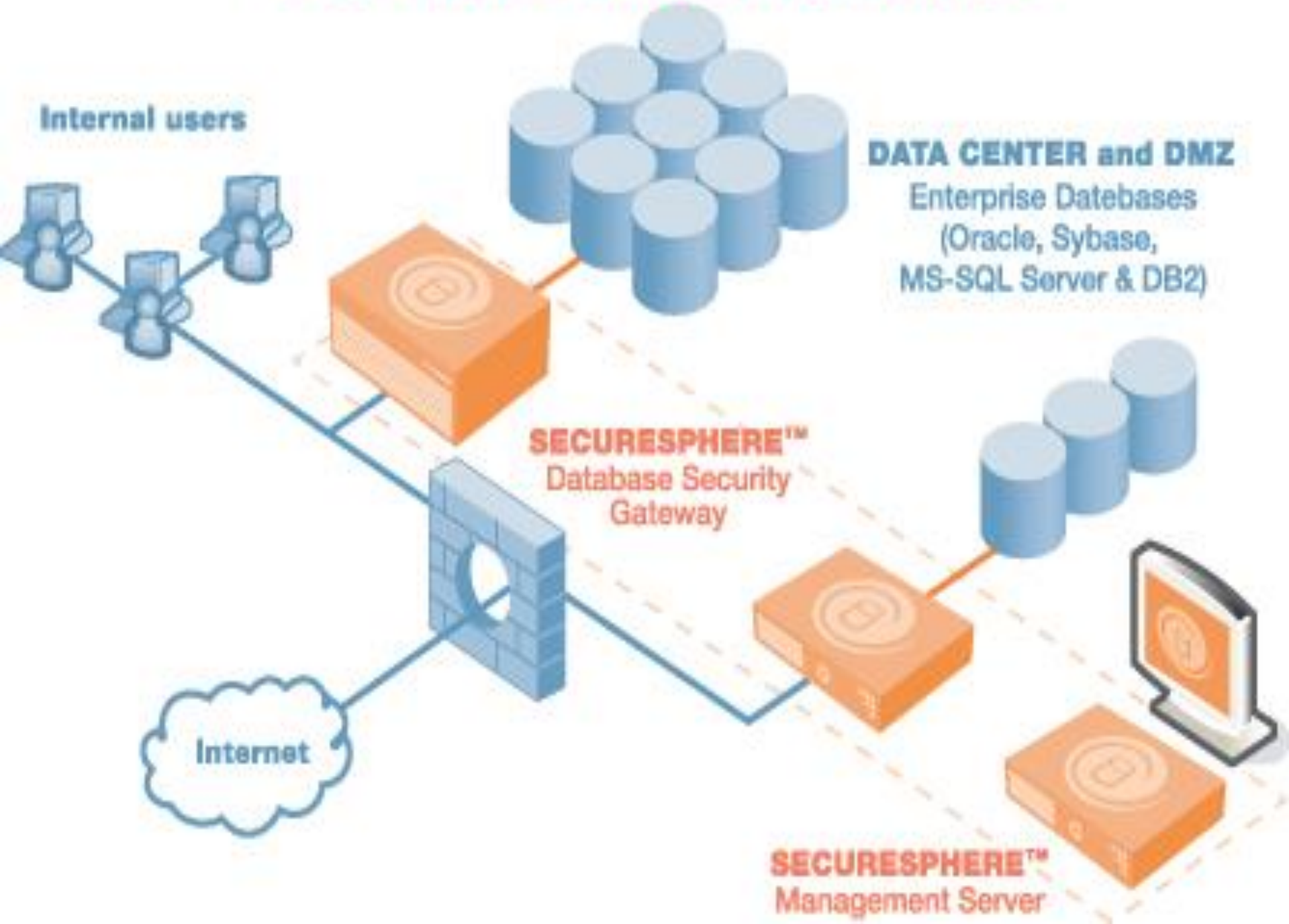
ការរក្សាសន្តិសុខរបស់ប្រព័ន្ធទិន្នន័យ (Database Security)

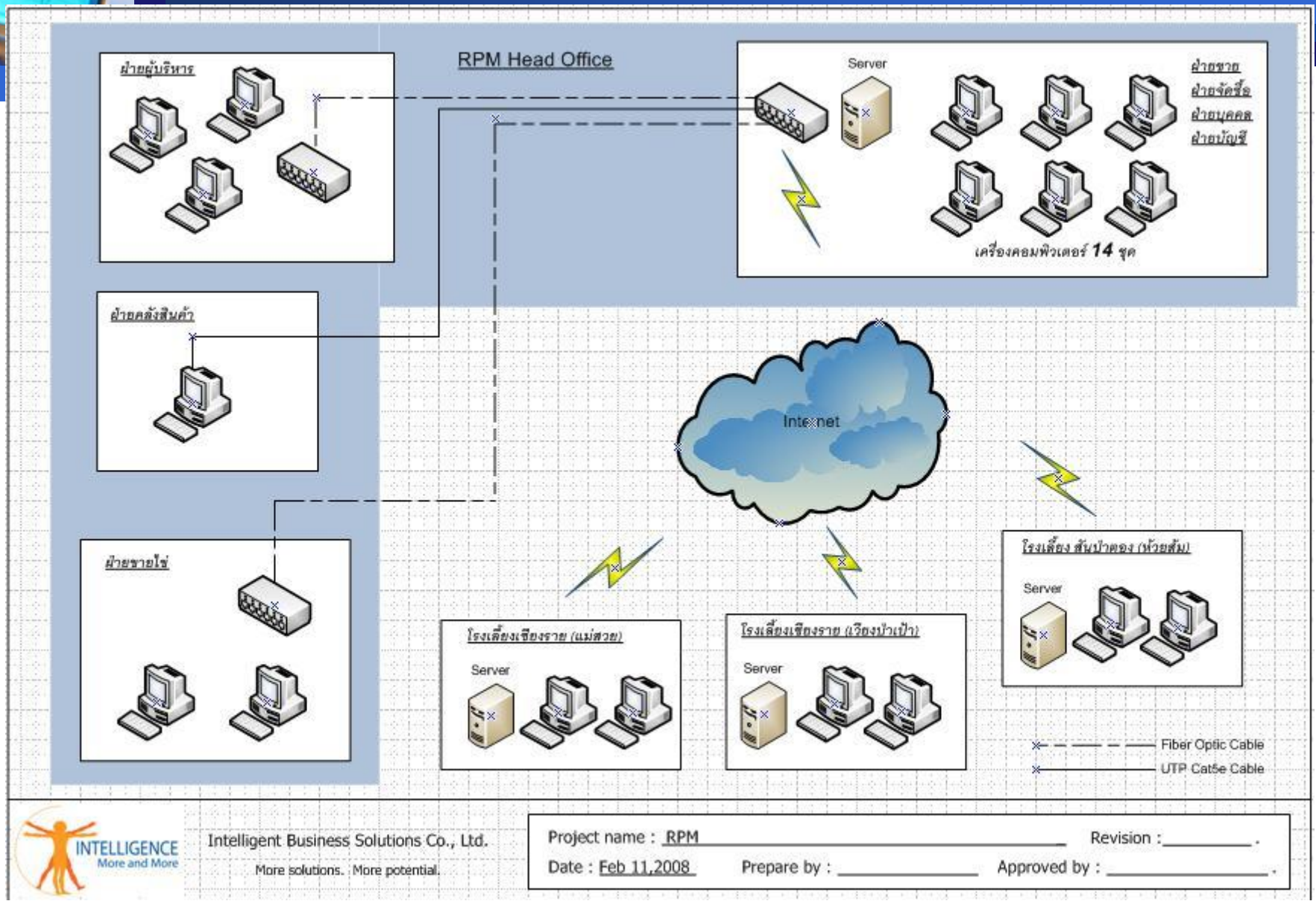
- ប្រព័ន្ធទិន្នន័យមានសារៈសំខាន់សម្រាប់ការការពារសុវត្ថិភាពទិន្នន័យ។ ដោយសារតែព័ត៌មាននៅក្នុងប្រព័ន្ធព័ត៌មានបណ្តាញបច្ចុប្បន្នភាគច្រើនត្រូវបានរក្សាទុកនៅក្នុងdatabase។ ពេលខ្លះសម្រាប់ភាពងាយស្រួលនៃការប្រើប្រាស់database វាជាចាំបាច់សម្រាប់មនុស្សច្រើននាក់ក្នុងការចូលប្រើទិន្នន័យក្នុងពេលដំណាលគ្នាពីទីតាំងផ្សេងគ្នា ឬជួនកាលវាចាំបាច់ក្នុងការប្រើប្រាស់បច្ចេកវិទ្យា Internet ដើម្បីភ្ជាប់ និងចែករំលែកព័ត៌មានជាទ្រង់ទ្រាយធំ។

Database Attack

- ការវាយប្រហារទៅលើប្រព័ន្ធទិន្នន័យដែលនឹងបង្កើតព័ត៌មានសម្ងាត់ បង្ហាញដល់ជនដែលគ្មានការអនុញ្ញាត
- ការវាយប្រហារលើទិន្នន័យធ្វើឱ្យទិន្នន័យដែលរក្សាទុកក្នុងត្រូវបានខូច។
- ការវាយប្រហារទៅលើប្រព័ន្ធទិន្នន័យ បង្ហាញព័ត៌មានដែលរក្សាទុកក្នុងប្រព័ន្ធទិន្នន័យមិនអាចចូលទៅបានទេ ទាល់តែមានការអនុញ្ញាតជាមុនសិន។

SECURESPHERE™ NETWORK ARCHITECTURE




RPM Head Office
ฝ่ายผู้บริหาร
Server
ฝ่ายขาย
ฝ่ายจัดซื้อ
ฝ่ายบุคคล
ฝ่ายบัญชี
เครื่องคอมพิวเตอร์ 14 ชุด
ฝ่ายคลังสินค้า
Internet
ฝ่ายขายไข่
โรงเลี้ยงเชียงราย (แม่สวย)
Server
โรงเลี้ยงเชียงราย (เวียงป่าเป้า)
Server
โรงเลี้ยง สันป่าตอง (ห้วยส้ม)
Server
Fiber Optic Cable
UTP Cat5e Cable
INTELLIGENCE
More and More
Intelligent Business Solutions Co., Ltd.
More solutions. More potential.
Project name : RPM
Revision :
Date : Feb 11,2008
Prepare by :
Approved by :

បញ្ហាប្រឈមនឹងការលេចធ្លាយទិន្នន័យពីការវិភាគទិន្នន័យ
(Inference Problem)

- ជាទូទៅ សុវត្ថិភាពនៃព័ត៌មាននោះ។ វាអាចត្រូវបានធ្វើដោយ បញ្ជាក់ថាការចូលប្រើព័ត៌មានអាចត្រូវបានចូលប្រើដោយសាធារណៈជនទូទៅ (Public) ឬអាចចូលបានតែដោយបុគ្គល(Personal/Private)
- ព័ត៌មានផ្ទាល់ខ្លួនសម្ងាត់ នឹងមិនអាចចូលប្រើបានសម្រាប់សាធារណជនទូទៅ ប៉ុន្តែព័ត៌មាននេះអាចត្រូវបានបែកធ្លាយដោយការវិភាគទិន្នន័យសាធារណៈ។
- ដូចជាមូលដ្ឋានទិន្នន័យនៅក្នុងនាយកដ្ឋានធនធានមនុស្ស

បញ្ហានៃការលេចធ្លាយព័ត៌មានសម្ងាត់ពីការប្រមូលព័ត៌មានផ្សេងៗដែលមិនអាចចូលគ្នាបាន (Database Aggregation Problem)

- បញ្ហានេះកើតឡើងនៅពេលប្រមូលព័ត៌មានផ្សេងៗ។ ដែលមិនមែនជាព័ត៌មានសម្ងាត់រួមគ្នា អាចបញ្ចូលគ្នាបានរហូតកើតមានព័ត៌មានសម្ងាត់អាចបែកធ្លាយ។
- ដំណោះស្រាយដែលយកមកប្រើ ការផ្លាស់ប្តូរបំណែងចែកថ្នាក់នៃព័ត៌មានមិនសម្ងាត់ តើនៅពេលណាដែលព័ត៌មានទាំងនេះ នៅពេលដែលវាត្រូវបានបញ្ចូល វាត្រូវបានផ្លាស់ប្តូរទៅជាកម្រិតនៃព័ត៌មានសម្ងាត់ដែលមិនអាចចូលទៅដល់មនុស្សដែលគ្មានការអនុញ្ញាត។

ប្រព័ន្ធទិន្នន័យគឺផ្អែកលើប្រព័ន្ធប្រតិបត្តិការដែលមានសុវត្ថិភាព (Database Applications on Secure Operating system)

- វិធីសាស្ត្រដ៏ល្អមួយចំពោះសុវត្ថិភាពទិន្នន័យជាមូលដ្ឋានគឺការប្រើប្រាស់កម្មវិធីទិន្នន័យនៅលើប្រព័ន្ធប្រតិបត្តិការដែលមានសុវត្ថិភាពខ្ពស់(Trusted Computing Base) វិធីសាស្ត្រនេះអាចផ្តល់នូវសុវត្ថិភាពសម្រាប់ទិន្នន័យ ពីព្រោះប្រព័ន្ធប្រតិបត្តិការអនុវត្តការងារផ្សេងៗដែលទាក់ទងនឹងការរក្សាទិន្នន័យស្ទើរតែទាំងអស់។ ទិន្នន័យត្រូវបានការពារដោយប្រព័ន្ធប្រតិបត្តិការដែលមានសុវត្ថិភាពខ្ពស់។

aixps2 - Microsoft Virtual PC 2007

Action Edit CD Floppy Help

```
IBM AIX PS/2 Operating System - Version 1.3.0
5713-AEQ (C) COPYRIGHT IBM CORP. 1988,1989,1990,1992
LICENSED MATERIAL - PROGRAM PROPERTY OF IBM
aixps2
Console login:root
                                — IBM AIX —

 ********************************************************************************
 *                                                                              *
 *              (      place your message of the day here      )                *
 *                                                                              *
 ********************************************************************************


aixps2 # uname -a
aix aixps 1 3.0 i386
aixps2 # _
```

ការធានាសុវត្ថិភាពប្រព័ន្ធទិន្នន័យដោយប្រើវិធីសាស្ត្រ Integrity Lock

- ការធានាសុវត្ថិភាពនេះអាចសម្រេចបានដោយប្រើ Trusted Front End (TFE) សម្រាប់ប្រើប្រាស់ក្នុងសុវត្ថិភាពនៃប្រព័ន្ធ database ដែល TFE វានឹងក្លាយជាអាជ្ញាកណ្តាលរវាងទិន្នន័យ និងកម្មវិធីផ្សេងទៀត។ ដើម្បីប្រើទិន្នន័យដែលជាកម្មវិធីដែលមិនគួរឱ្យទុកចិត្តទាក់ទងនឹងសុវត្ថិភាពក៏ថាបាន។

- **ការកំណត់សិទ្ធិចូលប្រើ**
- ការអនុញ្ញាតការចូលប្រើទិន្នន័យគឺជាពាក្យបញ្ជាដែលប្រើដើម្បីផ្តល់ការអនុញ្ញាតដល់អ្នកប្រើប្រាស់នីមួយៗ ដែលមានសិទ្ធិធ្វើសកម្មភាពលើទិន្នន័យក្នុងតារាងជាក់លាក់ ឬផ្តល់សិទ្ធិចូលប្រើទិន្នន័យតែប៉ុណ្ណោះ។
- (1) ការកំណត់សិទ្ធិចូលប្រើទិន្នន័យ ដូចជាការទាញយកទិន្នន័យដោយពាក្យបញ្ជា (SELECT) ការបន្ថែមទិន្នន័យដោយពាក្យបញ្ជា (INSERT) ការលុបទិន្នន័យដោយពាក្យបញ្ជា (DELETE) ឬការធ្វើបច្ចុប្បន្នភាពជាមួយពាក្យបញ្ជា (UPDATE)
- រូបបែបGRANT <SELECT,INSERT,UPDATE,DELETE> ON <ឈ្មោះ តារាង> TO <ឈ្មោះ អ្នកប្រើ>;
- (2)ផ្តល់សិទ្ធិចូលប្រើព័ត៌មានទាំងអស់។

  ប្រើ ALL PRIVILEGES (ឬ ALL ប៉ុណ្ណោះ)ក្នុងពាក្យបញ្ជា GRANT

  រូបបែប GRANT ALL ON <ឈ្មោះ តារាង > TO <ឈ្មោះ អ្នកប្រើ >;
- (3) ផ្តល់សិទ្ធិរុករកដល់អ្នកប្រើប្រាស់ទាំងអស់។
- ប្រើ PUBLIC ជាមួយ SELECT គួបជាមួយGRANT ។
- រូបបែប GRANT SELECT ON <table name> TO PUBLIC;

អ្វីដែលត្រូវពិចារណានៅពេលនាំយកប្រព័ន្ធ Database យកមកប្រើប្រាស់សម្រាប់សុវត្ថិភាពទិន្នន័យ

- កម្មវិធីបន្ថែមពីក្រុមហ៊ុនផលិតត្រូវតែត្រូវបានដំឡើងជានិច្ចដើម្បីការពារការខ្វះចន្លោះសុវត្ថិភាពណាមួយ។ ដែលអាចកើតឡើង
- ត្រូវតែសិក្សា និងធ្វើតាមយ៉ាងតឹងរឹងនូវការណែនាំដែលភ្ជាប់មកជាមួយសៀវភៅដៃដែលប្រើប្រាស់ប្រព័ន្ធទិន្នន័យសម្ងាត់។
- អ្នកគួរតែប្រើប្រព័ន្ធទិន្នន័យដែលត្រូវបានបញ្ជាក់ដោយស្តង់ដារយោធា (សហរដ្ឋអាមេរិក) ព្រោះវាជាស្តង់ដារសុវត្ថិភាពខ្ពស់ណាស់។

វិញ្ញាបនប័ត្រសុវត្ថិភាពប្រព័ន្ធមូលដ្ឋានទិន្នន័យដោយប្រើស្តង់ដារ TCSEC

- TCSEC(**Trusted Computer System Evaluation Criteria**) វាគឺជាស្តង់ដារដែលប្រើដើម្បីពណ៌នាអំពីកម្រិតសុវត្ថិភាពរបស់ប្រព័ន្ធមូលដ្ឋានទិន្នន័យ។ មានកម្រិតជាច្រើនអាស្រ័យលើការប្រើប្រាស់។ កម្រិតសុវត្ថិភាពគ្រប់គ្រាន់សម្រាប់ការប្រើប្រាស់ក្នុងអាជីវកម្មជារឿយៗជាកម្រិត C2 ដែលជារឿយៗគ្រប់គ្រាន់សម្រាប់តម្រូវការទូទៅ។ ប៉ុន្តែប្រសិនបើតម្រូវការសុវត្ថិភាពខ្ពស់ជាងនេះ ប្រព័ន្ធ B1 អាចត្រូវបានប្រើប្រាស់ ដែលជាកម្រិតសុវត្ថិភាពខ្ពស់ជាងច្រើន។

កម្រិតស្តង់ដារដែលប្រើសម្រាប់សុវត្ថិភាពនៃប្រព័ន្ធមូលដ្ឋានទិន្នន័យដែលមានតាមទីផ្សារទូទៅ

Database	Level	Certificate Date	Notes
Informix	B1	15/11/94	
Trusted oracle 7	B1	05/04/94	
Secure SQL Server, V11.0	B1	18/05/95	Sybase
SQL Server, V11.0.6	C2	13/10/95	Sybase
Informix Online/Secure 5.0	C2	13/10/94	

របៀបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ

- Salami Techniqueវាគឺជាវិធីសាស្ត្របណ្តើរៗនៃការកេងបន្លំប្រាក់ទំនិញ ឬសេវាកម្មពីប្រភពជាច្រើន។ យូរៗទៅចំនួនទឹកប្រាក់នេះនឹងកើនឡើង។

ឧទាហរណ៍ អ្នកក្លែងបន្លំអាចប្រើការបញ្ជាទិញដែលលាក់ដើម្បីកាត់បន្ថយចំនួនប្រាក់លើគណនីរបស់ពួកគេក្នុងខ្ទង់បីក្បៀសទៅ ដើម្បីសន្សំនៅក្នុងគណនីរបស់អ្នកបោកប្រាស់ដែលនឹងកើនឡើងរហូតដល់ចំនួនប្រាក់ច្រើនសន្ធឹកសន្ធាប់នៅទីបញ្ចប់។

រូបបៃបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Superzappingវាគឺជាអំពើពុករលួយដែលមានឈ្មោះតាមកម្មវិធីឧបករណ៍ប្រើប្រាស់ដែលមាននៅក្នុងប្រព័ន្ធកម្មវិធី IBM ។ កម្មវិធីអាចត្រូវបានប្រើដើម្បីធ្វើបច្ចុប្បន្នភាព ឬរុករកគ្រប់ផ្នែកទាំងអស់នៃប្រព័ន្ធ។ និងអាចកែលម្អធាតុមួយចំនួនដោយមិនចាំបាច់បង្កើតភស្តុតាងដើម្បីត្រួតពិនិត្យ។

  ឧទាហរណ៍ ការប្រើប្រាស់កម្មវិធីដើម្បីដកប្រាក់ទៅគណនីដៃគូអាជីវកម្មដោយមិនបង្កើតភស្តុតាងសវនកម្មនៅក្នុងសៀវភៅកត់ត្រា។

រូបបែបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Trap Doorsវាជាកូដកម្មវិធីដែលអនុញ្ញាតឱ្យអ្នកអភិវឌ្ឍន៍ជួសជុលកំហុសនៅពេលក្រោយ។ ជាធម្មតានៅក្នុងការពិនិត្យចុងក្រោយលេខកូដត្រូវតែដកចេញពីកម្មវិធី។ ប៉ុន្តែពេលខ្លះវាអាចត្រូវបានគេមិនអើពើដោយចៃដន្យ។ ឬមានបំណងរក្សាទុកនៅនឹងកន្លែង ដើម្បីភាពងាយស្រួលនៃការកែសម្រួលនៅពេលក្រោយ

  ឧទាហរណ៍ កម្មវិធីបំបាំងកាយប្រើពេលវេលា។ ឬការប្រើប្រាស់កម្មវិធីសម្ងាត់សម្រាប់នាយកប្រតិបត្តិ។

រូបបៃបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Logic Bombs គឺជាកម្មវិធីដែលអនុវត្តសកម្មភាពជាក់លាក់នៅលើប្រព័ន្ធកុំព្យូទ័រនៅពេលខ្លះ និងក្រោមលក្ខខណ្ឌ ឬកាលៈទេសៈអំណោយផលសម្រាប់អ្នកបោកប្រាស់។

  ឧទាហរណ៍ ការលាក់ពាក្យបញ្ជាដើម្បីពិនិត្យមើលឆ្នាំ កាលបរិច្ឆេទ និងពេលវេលានៅក្នុងប្រព័ន្ធកុំព្យូទ័រ នៅពេលដែលពេលវេលាពិតកំណត់ដោយអ្នកលាក់។ Logic Bombs ដឹកនាំឧបករណ៍កុំព្យូទ័រឱ្យដំណើរការដូចបំណង។

របៀបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Asynchronous Attacksវាគឺជាប្រភេទនៃកម្មវិធីដែលចាប់ផ្តើមនៅពេលដែលវាទទួលបានសញ្ញាបង្ហាញពីលទ្ធផលនៃប្រតិបត្តិការពីមុន។

- ឧទាហរណ៍នៅពេលណាមួយមានបញ្ហាឲ្យប្រព័ន្ធកុំព្យូទ័រធ្វើរបាយការណ៍អំពីលទ្ធផលការងារច្រើនក្នុងពេលតែមួយ។ បន្ទាប់ពីការចេញរបាយការណ៍បានផ្តល់ឱ្យត្រូវបានបញ្ចប់។

របៀបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Seavergingសំដៅលើការនាំចេញទិន្នន័យពីប្រព័ន្ធកុំព្យូទ័រ ដែលលេចឡើងក្នុងទម្រង់អាចមើលឃើញដោយភ្នែកទទេ ឬបន្តនៅក្នុងប្រព័ន្ធកុំព្យូទ័របន្ទាប់ពីការងារត្រូវបានដំណើរការដោយជោគជ័យ។

- ឧទាហរណ៍ ការទទួលទិន្នន័យដែលមិនទាន់សម្រេចនៅលើប្រព័ន្ធកុំព្យូទ័រដែលបណ្តាលមកពីការលុបតម្លៃមិនពេញលេញមិនអស់ដូចជាទិន្នន័យប្រាក់ខែជាដើម។

របៀបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Data Leakageវាជាការដកយកព័ត៌មានចេញពីប្រព័ន្ធកុំព្យូទ័រ។ តាមរយៈវិធីសាស្ត្រផ្សេងៗ អ្នកបោកប្រាស់អាចលាក់បច្ចេកទេសរបស់ពួកគេនៅក្នុងប្រព័ន្ធកុំព្យូទ័រ។ ប៉ុន្តែនៅក្នុងដំណើរការនៃការយកចេញទិន្នន័យមិនមានការសង្ស័យរបស់ប្រតិបត្តិករកុំព្យូទ័រឬបុគ្គលិកផ្សេងទៀត។

ឧទាហរណ៍ កុំព្យូទ័រត្រូវបានបំពាក់ដោយឧបករណ៍បញ្ជូនវិទ្យុតូចមួយ។ ឧបករណ៍បញ្ជូនអាចបង្ហាញព័ត៌មានដែលមាននៅក្នុងប្រព័ន្ធទៅកាន់ម៉ាស៊ីនដែលនៅឆ្ងាយ។

រូបបៃបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Piggybackingគឺជាការលុកលុយតាមរយៈឧបករណ៍អេឡិចត្រូនិក

- ឧទាហរណ៍ ការភ្ជាប់ខ្សែទូរស័ព្ទដូចគ្នាដោយសម្ងាត់ នៅពេលដែលម៉ាស៊ីនពិតត្រូវបានបើកចូលទៅក្នុងប្រព័ន្ធ ដែលអាចមានលេខកូដសម្ងាត់ ក្នុងអំឡុងពេលដែលអ្នកប្រើប្រាស់ពិតប្រាកដបានចូលហើយប្រហែលជាមិននៅក្នុងម៉ាស៊ីនមួយរយៈ ដូច្នេះអាចប្រតិបត្តិការក្លែងបន្លំបាន ។

រូបបៃបក្លែងបន្លំនៅក្នុងប្រព័ន្ធបណ្តាញ (ត)

- Wiretappingសំដៅទៅលើការក្លែងបន្លំដោយការកែប្រែទិន្នន័យដោយខុសច្បាប់តាមទម្រង់ផ្សេងៗក្នុងការទំនាក់ទំនងកំឡុងពេលទទួល និងបញ្ជូនទិន្នន័យ។

- ប្រភេទនៃការក្លែងបន្លំនេះមិនមានការពេញនិយមទេព្រោះវាពិបាកក្នុងការធ្វើ។ ដោយសារតែឧបករណ៍នេះត្រូវបានទាមទារដើម្បីកត់ត្រា និងបោះពុម្ពទិន្នន័យ។ វាក៏មានវិធីសាស្ត្រផ្សេងទៀតដែលងាយស្រួលក្នុងការក្លែងបន្លំ។

គោលការណ៍ណែនាំសម្រាប់ការគ្រប់គ្រងប្រព័ន្ធព័ត៌មាននៅលើបណ្តាញInternet

- Firewall វាគ្រប់គ្រង និងត្រួតពិនិត្យទិន្នន័យដែលឆ្លងកាត់បណ្តាញខាងក្នុង និងទិន្នន័យចេញទៅបណ្តាញខាងក្រៅ។ ច្បាប់ផ្សេងៗត្រូវបានបង្កើតឡើងដើម្បីធានាថាទិន្នន័យនឹងឆ្លងកាត់បណ្តាញ។
- Cryptologyមាន
  - ការចាក់សោកូដ (Encryption)វាធ្វើឱ្យទិន្នន័យដែលបានបញ្ជូនតាមបណ្តាញក្នុងទម្រង់ដែលមិនអាចអានបាន និងធ្វើដោយសម្ងាត់។
  - ការដោះសោកូដ (Decryption)វាបំប្លែងទិន្នន័យដែលបាន Encryptionត្រឡប់មកវិញដើម្បីអាចអានបាន។

ឧទាហរណ៍នៃការចាក់សោកូដ និងការដោះសោកូដ

- ការប្រើប្រាស់ចុះហត្ថលេខាឌីជីថលសម្រាប់ការត្រួតពិនិត្យ និងការផ្ទៀងផ្ទាត់(Digital Signature)ដំណើរការគឺដូចខាងក្រោម៖
  - ការនាំទិន្នន័យអេឡិចត្រូនិចចូល ការប្រើប្រាស់សោឯកជនរបស់អ្នកផ្ញើ (Private Key) ដែលប្រៀបដូចជាហត្ថលេខារបស់អ្នកផ្ញើ ព្រោះមានតែអ្នកផ្ញើប៉ុណ្ណោះដែលមានសោឯកជនរបស់អ្នកផ្ញើ។ ហើយនឹងទទួលបានទិន្នន័យដែលបានEncryption វាត្រូវបានគេហៅថាហត្ថលេខាឌីជីថល។
  - ផ្ញើហត្ថលេខាឌីជីថលជាមួយព័ត៌មានដើមទៅអ្នកទទួល។ បន្ទាប់មកយកហត្ថលេខាឌីជីថលដើម្បីDecryptionដោយប្រើសោសាធារណៈរបស់អ្នកផ្ញើ។

គោលការណ៍ណែនាំការប្រើប្រាស់Internetក្នុងសវនកម្ម

- សវនករប្រើប្រាស់Internetសម្រាប់ជាប្រយោជន៍នៃសវនកម្មតាមពីរវិធី៖
- ការចូលប្រើទិន្នន័យ - សវនករអាចចូលប្រើប្រព័ន្ធព័ត៌មានសាធីវកម្ម ដើម្បីចូលប្រើព័ត៌មានណាមួយដែលពួកគេត្រូវការតាមរយៈInternet និងអាចប្រើព័ត៌មានទាំងនោះសម្រាប់ការធ្វៀងផ្ទាត់ ។
- ការត្រួតពិនិត្យជាបន្តបន្ទាប់ - សវនករអាចត្រូវបានកំណត់ឱ្យមានការជូនដំណឹងដោយស្វ័យប្រវត្តិនៅពេលដែលប្រតិបត្តិការមិនធម្មតា ឬព្រឹត្តិការណ៍មិនធម្មតាកើតឡើងនៅក្នុងប្រព័ន្ធព័ត៌មាន ។ អាចធ្វើសវនកម្មប្រព័ន្ធព័ត៌មានជាបន្តបន្ទាប់ដោយមិនចាំបាច់ស្នើសុំការត្រួតពិនិត្យរាល់ពេល និងអាចដោះស្រាយបញ្ហាបានទាន់ពេលវេលា

គោលការណ៍ណែនាំការប្រើប្រាស់Internetក្នុងសវនកម្ម

Internetបានណែនាំវិធីសាស្ត្រថ្មីនៃការធ្វើងផ្ទាត់ដូចខាងក្រោម:

- កុំព្យូទ័រអាចត្រូវបានត្រួតពិនិត្យដោយមិនចាំបាច់នៅលើប្រព័ន្ធអនឡាញតែមួយ។
- ឯកសារដោទម្រង់អេឡិចត្រូនិក (Soft File) អាចត្រូវបានពិនិត្យដោយសវនករពីគ្រប់ទីតាំង។
- អាចពិនិត្យម៉ាស៊ីនកុំព្យូទ័រតាមរយៈInternet
- អនុញ្ញាតឱ្យសវនករបន្តសវនកម្ម ជំនួសឱ្យការស្នើសុំសវនកម្មម្តងម្កាល។

សវនកម្មសុវត្ថិភាពផ្អែកលើបណ្តាញ

- ឯកសារសវនកម្ម គឺជាឯកសារកុំព្យូទ័រដែលកត់ត្រាដោយស្វ័យប្រវត្តិនូវលំដាប់នៃព្រឹត្តិការណ៍ដែលកើតឡើងនៅក្នុងប្រព័ន្ធ ដើម្បីកត់ត្រាសកម្មភាពណាមួយដែលបានអនុវត្តនៅលើប្រព័ន្ធតាមលំដាប់លំដោយចាប់ពីដើមដល់ចប់ ។ និងកត់ត្រាពេលវេលាពីការចូលទៅក្នុងប្រព័ន្ធរហូតដល់ការចេញពីប្រព័ន្ធ

  ឯកសារតាមដានសវនកម្មត្រូវបានបែងចែកជាពីរប្រភេទ៖

  - សវនកម្មគណនេយ្យ(Accounting Audit Trail)
  - សវនកម្មប្រតិបត្តិការ(Operation Audit Trail)

សវនកម្មសុវត្ថិភាពផ្នែកលើបណ្តាញ

- ការគ្រប់គ្រងអត្ថិភាព - គ្រប់គ្រងការបម្រុងទុក និងការស្តារបណ្តាញឡើងវិញ។ មានវិធីសាស្ត្រផ្សេងៗគ្នា រួមមាន:
- ផ្តល់កន្លែង និងរក្សាទុកឧបករណ៍ និងផ្នែកទាំងអស់ដែលនឹងត្រូវការនៅក្នុងបណ្តាញដែលលែងត្រូវការតទៅទៀត។
- ប្រើឧបករណ៍ដែលមានសមត្ថភាពដោះស្រាយកំហុសដែលអាចកើតឡើងនៅក្នុងបណ្តាញ។
- ប្រើឧបករណ៍ដែលត្រូវបានសាកល្បងថាមានគុណភាពខ្ពស់។
- មានការថែទាំhardware និងsoftware គ្រប់គ្រាន់ និងទៀងទាត់។
- មានកន្លែងស្តារឡើងវិញ និងសមហេតុផល។

ការគ្រប់គ្រងហានិភ័យបច្ចេកវិទ្យាព័ត៌មាន

ការគ្រប់គ្រងហានិភ័យ(Risk Management) គឺជាដំណើរការនៃការកំណត់អត្តសញ្ញាណ វិភាគ វាយតម្លៃ ត្រួតពិនិត្យ តាមដាន និងគ្រប់គ្រងហានិភ័យដែលទាក់ទងនឹងសកម្មភាព។ មុខងារ និងដំណើរការការងារ ដើម្បីឱ្យស្ថាប័នកាត់បន្ថយការខូចខាតពីហានិភ័យតាមដែលអាចធ្វើទៅបាន។ ដោយសារតែគ្រោះថ្នាក់ដែលស្ថាប័នត្រូវប្រឈមមុខនៅពេលណាមួយ។

ដំណើរការគ្រប់គ្រងហានិភ័យបច្ចេកវិទ្យាព័ត៌មាន

- ដំណើរការគ្រប់គ្រងហានិភ័យចែកចេញជា ៦ ដំហានដូចខាងក្រោម៖
- 1. ការវាយតម្លៃហានិភ័យ(Risk assessment) វាមានដំណើរការវិភាគហានិភ័យ និង ការវាយតម្លៃហានិភ័យ
  - 1.1 ការវិភាគហានិភ័យ(Risk analysis) វាមាន 3 ដំហានដូចខាងក្រោម:
    - ▫ការកំណត់អត្តសញ្ញាណហានិភ័យ (Risk identification)
    - ▫ លក្ខណៈលម្អិតនៃហានិភ័យ(Risk description)
    - ▫ ការប៉ាន់ស្មានហានិភ័យ(Risk estimation)
  - 1.2 វាយតម្លៃហានិភ័យ(Risk evaluation)
- 2. របាយការណ៍លទ្ធផលការវិភាគហានិភ័យ(Risk reporting)
- 3. ដំណើរការកាត់បន្ថយហានិភ័យ(Risk mitigation)
- 4. ការគ្រប់គ្រងហានិភ័យ(Risk control)
- 5.របាយការណ៍ហានិភ័យសំណល់ (Residual risk reporting)
- 6. ការត្រួតពិនិត្យ(Monitoring)

Date 26 01 23

- ការធានាព័ត៌មានហានិភ័យមានពីរផ្នែក៖
  - ភាពងាយរងគ្រោះ(Vulnerability)
  - ការគំរាមកំហែង(Threat)
- ភាពងាយរងគ្រោះ(Vulnerability) សំដៅទៅលើឆានែលដែលអាចត្រូវបានប្រើសម្រាប់ការវាយប្រហារមួយដូចជាទ្វារចំហឬបង្អួច។ វាជាល្បិចដែលជនទុច្ចរិតអាចចូលលួចទ្រព្យសម្បត្តិក្នុងផ្ទះ។ ប្រសិនបើបច្ចេកវិទ្យាដូចជាការបើកportដែលមិនចាំបាច់ អាចមានគ្រោះថ្នាក់។

- ការគំរាមកំហែង(Threat)គឺជាអ្វីដែលអាចកើតឡើង និងបង្កគ្រោះថ្នាក់ដល់ទ្រព្យសម្បត្តិ
  - ការគំរាមកំហែងនៅក្នុងផ្ទះ ដូចជាការក្លែងបន្លំ ដំណើរការខុសប្រក្រតី
  - ការគំរាមកំហែងពីខាងក្រៅស្ថាប័ន ដូចជាការលួចចូលប្រព័ន្ធជាដើម។ ការបំផ្លិចបំផ្លាញ លួច ឬបោកបញ្ឆោតព័ត៌មាន
  - គ្រោះធម្មជាតិដូចជា ទឹកជំនន់ រញ្ជួយដី រលកយក្សស៊ូណាមិ អគ្គីភ័យ រន្ទះ
  - ការគំរាមកំហែងបរិស្ថានដែលមិនសមស្របដូចជាការលេចធ្លាយទឹក ធូលី សារធាតុគីមី សីតុណ្ហភាពក្តៅ សំណើម

ការវាយប្រហារ(Target)

- គោលដៅវាយប្រហារ
  - សម្ងាត់ (Confidentiality)វាត្រូវបានកំណត់គោលដៅតែនៅពេលដែលការសម្ងាត់នៃព័ត៌មានត្រូវបានបង្ហាញ ដូចជាអាថ៌កំបាំងរបស់រដ្ឋាភិបាល អាថ៌កំបាំងអាជីវកម្ម ព័ត៌មានផ្ទាល់ខ្លួន។
  - ស្ថេរភាព(Integrity)នឹងត្រូវបានកំណត់គោលដៅនៅពេលព្យាយាមផ្លាស់ប្តូរទិន្នន័យ ឬបញ្ឆោតឱ្យជឿព័ត៌មានមិនពិត ដូចជាការផ្លាស់ប្តូរសមតុល្យនៅក្នុងគណនីធនាគារ ដើម្បីធ្វើឱ្យចំនួនទឹកប្រាក់កាន់តែច្រើន
  - ភាពអាចរកបាន(Availability)ត្រូវបានកំណត់គោលដៅជាមួយនឹងការបដិសេធនៃការវាយប្រហារសេវាកម្ម។ គោលដៅនោះអាចជាប្រព័ន្ធដែលផ្តល់សេវាទិន្នន័យ ឬទិន្នន័យរចនាសម្ព័ន្ធរបស់អង្គភាព។

អ្នកវាយប្រហារ

- គឺអ្នកណាម្នាក់ដែលធ្វើសកម្មភាពណាមួយដែលបណ្តាលឱ្យមានផលវិបាកអវិជ្ជមានជាមួយអ្នកវាយប្រហារ លក្ខណៈពិសេសនៃអ្នកវាយប្រហារ
  - ភាពងាយស្រួល(Access) អាចទៅដល់គោលដៅ ចូលទៅកាន់ប្រព័ន្ធ បណ្តាញ ទីតាំង ឬព័ត៌មានដែលចង់បាន ឧទាហរណ៍អាចជាដោយផ្ទាល់ ការលួចចូលទៅក្នុងប្រព័ន្ធគណនី ឬដោយប្រយោល ជាឧទាហរណ៍ អាចមានឱកាសចូលប្រើដោយបណ្តាញពិសេស។ បុគ្គលិកភ្លេចបិទទ្វារដើម្បីលួចចូល។
  - ចំណេះដឹង (Knowledge) ចំណេះដឹងអំពីគោលដៅដូចជា គណនីអ្នកប្រើប្រាស់ ពាក្យសម្ងាត់ អាសយដ្ឋាន អាសយដ្ឋាន IP ប្រព័ន្ធសុវត្ថិភាព
  - ការលើកទឹកចិត្ត(Motivate) បញ្ហាប្រឈម, ចង់បាន, ដូចជាលុយ, របស់, សេវាកម្ម, ឬព័ត៌មាន។

- អ្នកវាយប្រហារមានដូចខាងក្រោម៖
  - បុគ្គលិក
  - បុគ្គលិកចាស់
  - Hacker
  - សត្រូវ ឬគូប្រជែង
  - ភេរវករ
  - អតិថិជន
  - គ្រោះធម្មជាតិ

ហេតុការកើតឡើង

- របៀបដែលអ្នកវាយប្រហារបង្កគ្រោះថ្នាក់ដល់ស្ថាប័នមួយ

ឧទាហរណ៍៖

- កែសម្រួលទំព័រគេហទំព័ររបស់ស្ថាប័ន។
- ការប្រើប្រាស់ខុស ឬលើសគណនីអ្នកប្រើប្រាស់ត្រូវបានអនុញ្ញាត។
- ការផ្លាស់ប្តូរព័ត៌មានដោយចេតនា ឬអចេតនា
- ការលួចចូលដោយគ្មានការអនុញ្ញាត
- ការបំផ្លាញប្រព័ន្ធដោយចៃដន្យ
- ការរំខានដល់ប្រព័ន្ធទំនាក់ទំនងខាងក្នុង និងខាងក្រៅ

ការវិភាគហានិភ័យ(Risk assessment)

- 1. ការវិភាគហានិភ័យ ការវិភាគហានិភ័យមាន ៣ ដំណាក់កាល៖
- ដំណាក់កាល 1ការកំណត់អត្តសញ្ញាណហានិភ័យ (Risk identification) វាបានចង្អុលបង្ហាញពីបញ្ហានៃភាពមិនប្រក្រតីរបស់អង្គការដែលកំពុងប្រឈមមុខ។ ដំណើរការនេះទាមទារការយល់ដឹងអំពីអង្គការ។ បេសកកម្ម និងសកម្មភាព បរិយាកាសផ្លូវច្បាប់ សង្គម នយោបាយ និងវប្បធម៌ ការអភិវឌ្ឍន៍ និងកត្តាដែលប៉ះពាល់ដល់ភាពជោគជ័យរបស់អង្គការ រួមទាំងឱកាស និងការគំរាមកំហែងដល់អង្គការ ការកំណត់អត្តសញ្ញាណហានិភ័យគួរតែត្រូវបានអនុវត្តយ៉ាងទូលំទូលាយនៅគ្រប់សកម្មភាពទាំងអស់។ ភាគីសាជីវកម្ម មូលហេតុចម្បងនៃហានិភ័យគឺវត្តមាននៃការគំរាមកំហែង ។(Threat) ដែលអាចបណ្តាលឱ្យមានការរំលោភលើសុវត្ថិភាពព័ត៌មាន និងមានផលប៉ះពាល់ភ្ជាប់មកជាមួយ។

- ដំណាក់កាល 2 លក្ខណៈលម្អិតនៃហានិភ័យ(description of risk) នៅពេលដែលហានិភ័យត្រូវបានកំណត់ និងពិពណ៌នាលម្អិត និងលក្ខណៈនៃហានិភ័យដូចខាងក្រោម៖
  - - ឈ្មោះហានិភ័យ(Name)
  - -វិសាលភាព (Scope)
  - - លក្ខណៈហានិភ័យ(Nature)
  - -មនុស្សដែលរងផលប៉ះពាល់
  - - លក្ខណៈការប៉ាន់ស្មាន
  - - ការទទួលស្គាល់ហានិភ័យ
  - -ការព្យាបាលនិងការគ្រប់គ្រង
  - - ការណែនាំអំពីការកែលម្អ
  - - ការអភិវឌ្ឍន៍យុទ្ធសាស្ត្រ និងគោលនយោបាយ

- ដំណាក់កាល 3ការប៉ាន់ស្មានហានិភ័យ (risk estimation)ជំហាននេះគឺដើម្បីពិនិត្យមើលបញ្ហាហានិភ័យទាក់ទងនឹងលទ្ធភាពនៃឧប្បត្តិហេតុ (incident) ឬព្រឹត្តិការណ៍(event) ថាតើផលប៉ះពាល់ធ្ងន់ធ្ងរ ឬខូចខាតប៉ុណ្ណា ?

- ឱកាស ឬប្រូបាប(Probability or Likelihood) ឬភាពញឹកញាប់នៃការកើតឡើង ឬព្រឹត្តិការណ៍ វាអាចបែងចែកជា 5 ដំណាក់កាលពីឡើងទៅចុះ
  - - ញឹកញាប់(frequent)ជាញឹកញាប់ត្រូវបានរកឃើញនៅលើមូលដ្ឋានធម្មតា ។
  - -ប្រសព្វ (probable)
  - - ដោយចៃដន្យ(occasional)
  - - កម្រណាស់ ។(remote)
  - - ស្ទើរតែមិនដែល(improbable)

- <u>ចំណាំ ៖ អង្គការមួយចំនួនបែងចែកភាពញឹកញាប់នៃឧប្បត្តិហេតុជា 3 ដំណាក់កាលតែប៉ុណ្ណោះ អាស្រ័យលើតម្រូវការ និងភាពសមស្របរបស់ស្ថាប័ននីមួយៗ ។</u>

1.2ការវាយតម្លៃហានិភ័យ (Risk evaluation)

- ការវិនិច្ឆ័យទទួលយកហានិភ័យ(Risk acceptance criteria) តើអាចទទួលយកបានប៉ុន្មាន ដើម្បីជួយសម្រេចចិត្តពីរបៀបការពារហានិភ័យនោះបន្ថែមទៀត ពិចារណាទៅលើ
  - - ការចំណាយ អត្ថប្រយោជន៍ និងប្រសិទ្ធភាពនៃការកាត់បន្ថយហានិភ័យ (costs and benefits)
  - - តម្រូវការផ្នែកច្បាប់ និងបទប្បញ្ញត្តិរបស់អង្គការ(legal requirements)
  - - កត្តាសេដ្ឋកិច្ចសង្គម(socioeconomic factors)
  - - កត្តាបរិស្ថាន(environmental factors)
  - -បញ្ហាសំខាន់ៗពីទស្សនៈរបស់អ្នកពាក់ព័ន្ធ (concerns of stakeholders)

ตัวอย่าง การประเมินค่าความเสี่ยง (risk evaluation)

- តារាងបង្ហាញពីម៉ាទ្រីសកម្រិតហានិភ័យ3x3

โอกาสการเกิดความเสี่ยง (Likelihood)	ความรุนแรงของความเสี่ยง (Impact)		
	ต่ำ (10)	ปานกลาง (50)	สูง (100)
สูง (1.0)	ต่ำ 10 x 1.0 = 10	ปานกลาง 50 x 1.0 = 50	สูง 100 x 1.0 = 100
ปานกลาง (0.5)	ต่ำ 10 x 0.5 = 5	ปานกลาง 50 x 0.5 = 25	ปานกลาง 100 x 0.5 = 50
ต่ำ (0.1)	ต่ำ 10 x 0.1 = 1	ต่ำ 50 x 0.1 = 5	ต่ำ 100 x 0.1 = 10

- ឧទាហរណ៍នៅទីនេះប្រើម៉ាទ្រីស 3x3 ពី 3 Threat Chance (ខ្ពស់ មធ្យម ទាប) និង 3 Threat Effects (ខ្ពស់ មធ្យម ទាប) ដែលបង្ហាញក្នុងតារាងខាងក្រោម។ ផលប៉ះពាល់នៃការគំរាមកំហែងមានតម្លៃស្មើរ 1 នៅខ្ពស់ តម្លៃស្មើរ 0.5 នៅកម្រិតមធ្យម និង តម្លៃស្មើ0.1 នៅកម្រិតទាប និងភាពធ្ងន់ធ្ងរនៃផលប៉ះពាល់ការគំរាមកំហែងនៅ,តម្លៃ 100 នៅពេលកម្រិតខ្ពស់ ,វាមានតម្លៃ 50 នៅពេលវាមានកម្រិតមធ្យម ,និង 10 នៅពេលវាទាប រៀងគ្នាតាមលំដាប់។

- កម្រិតហានិភ័យខ្ពស់មានន័យថា ត្រូវតែជួសជុលជាបន្ទាន់។ ប្រព័ន្ធដែលកំពុងដំណើរការអាចនៅតែដំណើរការជាធម្មតា ប៉ុន្តែផែនការជួសជុលត្រូវតែត្រូវបានអនុវត្តឱ្យបានឆាប់តាមដែលអាចធ្វើទៅបាន។
- កម្រិតហានិភ័យមធ្យម នេះមានន័យថា គួរតែមានការកែប្រែ ហើយផែនការត្រួតពិនិត្យគួរតែត្រូវបានធ្វើបច្ចុប្បន្នភាព ហើយបន្ទាប់មកទទួលយកហានិភ័យជាមុខងារនៃលទ្ធភាពនៃឧប្បត្តិហេតុណាមួយ។ ដែលបង្កការគំរាមកំហែងដល់ប្រព័ន្ធដែលខ្សោយដើម្បីការពារ ជាមួយនឹងភាពធ្ងន់ធ្ងរនៃផលប៉ះពាល់ដែលនឹងកើតឡើងពីការគំរាមកំហែងនោះ។
- កម្រិតហានិភ័យទាប នេះមានន័យថាប្រព័ន្ធគួរតែត្រូវបានធ្វើសវនកម្មដើម្បីធានាថាផែនការត្រួតពិនិត្យដែលមានស្រាប់អាចដោះស្រាយបញ្ហា និងដោះស្រាយហានិភ័យ។

2. របាយការណ៍លទ្ធផលការវិភាគហានិភ័យ(Risk reporting)

- នៅពេលដែលការវាយតម្លៃហានិភ័យត្រូវបានបញ្ចប់ ចាំបាច់ត្រូវចេញរបាយការណ៍វាយតម្លៃក្នុងឯកសារដែលអ្នកផ្សេងអាចអានបាន ។ ឯកសារនេះនឹងមានសារៈសំខាន់ក្នុងការទំនាក់ទំនងជាមួយបុគ្គលិកទូទាំងស្ថាប័ន ។ របាយការណ៍នេះមានយ៉ាងហោចណាស់ការពិពណ៌នាលម្អិតនៃទម្រង់ហានិភ័យ ។ ហើយការចេញរបាយការណ៍មានគោលបំណងធ្វើឱ្យផ្នែកខាងក្រោមយល់ដឹង

ផ្នែកគ្រប់គ្រង → ម្ចាស់គ្រប់គ្រង → អ្នកធ្វើការ

ផ្នែកគ្រប់គ្រង

ទទួលស្គាល់សារៈសំខាន់នៃហានិភ័យដែលប្រឈមមុខនឹងអង្គការ។

- ស្វែងយល់ពីផលប៉ះពាល់លើភាគីពាក់ព័ន្ធផ្សេងៗ ក្នុងករណីមានឧប្បត្តិហេតុកើតឡើង ឬព្រឹត្តិការណ៍ និងប៉ះពាល់យ៉ាងធ្ងន់ធ្ងរដល់បេសកកម្ម និងលទ្ធផលនៃប្រតិបត្តិការ
- ធ្វើសកម្មភាពដើម្បីបង្កើតការយល់ដឹងអំពីបញ្ហាហានិភ័យដែលត្រូវយល់ឃើញទូទាំងអង្គភាព។
- ស្វែងយល់ពីផលប៉ះពាល់ដែលអាចកើតមានលើទំនុកចិត្តរបស់អ្នកដែលរងផលប៉ះពាល់
- ធានាថាដំណើរការគ្រប់គ្រងហានិភ័យកំពុងដំណើរការប្រកបដោយប្រសិទ្ធភាព
- ចេញគោលនយោបាយគ្រប់គ្រងហានិភ័យដែលមានខ្លឹមសារស្តីពីទស្សនវិជ្ជា និងទំនួលខុសត្រូវរបស់នាយកដ្ឋាន និងបុគ្គលិកផ្សេងៗក្នុងការគ្រប់គ្រងហានិភ័យ។

ម្ចាស់គ្រប់គ្រង

- ដឹងពីហានិភ័យដែលទាក់ទងនឹងកាតព្វកិច្ចរបស់មនុស្សម្នាក់ ផលប៉ះពាល់ដែលអាចមានលើភ្នាក់ងារផ្សេងទៀត ឬសកម្មភាពផ្សេងទៀតនៅក្នុងអង្គភាព។
- មានសូចនាករការអនុវត្តនៃសកម្មភាពរបស់អង្គការដើម្បីដឹងថាតើប្រព័ន្ធការងារផ្ទាល់ខ្លួនរបស់ពួកគេរងផលប៉ះពាល់ដោយហានិភ័យកម្រិតណា។
- រាយការណ៍ពីផលប៉ះពាល់នៃហានិភ័យនៅក្នុងព្រឹត្តិការណ៍ ឬនឹងកើតឡើង ហើយរកដំណោះស្រាយ
- រាយការណ៍ពីហានិភ័យ ឬការបរាជ័យដែលកំពុងកើតមាន ក្នុងវិធានការដើម្បីគ្រប់គ្រង ឬទប់ស្កាត់ការឃុំឃាំងព័ត៌មានដែលមានស្រាប់

អ្នកប្រតិបត្តិ

-ស្វែងយល់ពីតួនាទី ទំនួលខុសត្រូវ និង ទំនួលខុសត្រូវនៃហានិភ័យនីមួយៗ

- ស្វែងយល់ពីតួនាទីនៃការកែលម្អជាបន្តបន្ទាប់ក្នុងការគ្រប់គ្រងហានិភ័យ

- យល់ដឹងពីការគ្រប់គ្រងហានិភ័យ និងការយល់ដឹងអំពីហានិភ័យរបស់អង្គភាពដ៏សំខាន់

3.ដំណើរការកាត់បន្ថយហានិភ័យ(Risk mitigation)

- ការកាត់បន្ថយហានិភ័យពាក់ព័ន្ធនឹងចំណាត់ថ្នាក់ ការគណនាហានិភ័យ និងអនុវត្តការត្រួតពិនិត្យកាត់បន្ថយហានិភ័យសមស្របដោយអនុលោមតាមគោលការណ៍ណែនាំដែលបានមកពីការវាយតម្លៃហានិភ័យ ដោយសារការលុបបំបាត់ហានិភ័យនៃប្រព័ន្ធទាំងអស់គឺពិបាក។ នាយកប្រតិបត្តិអាជីវកម្មទទួលខុសត្រូវចំពោះការងារនេះជាមួយនឹងសំណងថវិកាទាបបំផុត(Least-cost) និងប្រើប្រាស់វិធីសាស្ត្រត្រួតពិនិត្យសមស្របបំផុតដើម្បីកាត់បន្ថយកម្រិតហានិភ័យដល់កម្រិតដែលអាចទទួលយកបាន។ ដោយកាត់បន្ថយផលប៉ះពាល់លើបេសកកម្ម និងធនធានរបស់អង្គភាព។
- ជម្រើសសម្រាប់កាត់បន្ថយហានិភ័យ អាចចែកចេញជា ៦ ប្រភេទដូចខាងក្រោម៖

3.1 ការទទួលស្គាល់ហានិភ័យ(Risk Assumption)

- ការទទួលយកហានិភ័យដែលមានស្រាប់ និងអនុញ្ញាតឱ្យប្រព័ន្ធព័ត៌មានដំណើរការជាធម្មតា នេះគឺជាការទទួលយកនូវផលវិបាកដែលអាចកើតមាន ដូចជាការផ្ទៀងផ្ទាត់ដោយប្រើ ID និង Password វាមានហានិភ័យដោយសារតែចោរកម្មអាចត្រូវបានគេប្រើប្រាស់ (biometrics) ដូចជាពិនិត្យស្នាមម្រាមដៃ វាមានតម្លៃថ្លៃ មន្ទីរពេទ្យអាចទទួលយកហានិភ័យនៃប្រព័ន្ធបច្ចុប្បន្ន ហើយបន្តធ្វើការដោយមិនធ្វើអ្វីទាំងអស់។

3.2ការជៀសវាងហានិភ័យ (Risk Avoidance)

- ការជៀសវាងហានិភ័យដោយការលុបបំបាត់បុព្វហេតុនៃហានិភ័យ

ឧទាហរណ៍នៅពេលដែលគេរកឃើញថាមន្ទីរពេទ្យបច្ចុប្បន្ន មានការបម្រុងទុកមួយប៉ុណ្ណោះ ហើយត្រូវចាត់ថ្នាក់ជាហានិភ័យនៃការបាត់បង់។ ដើម្បីជៀសវាងហានិភ័យនេះរួមបញ្ចូលការបម្រុងទុកពីរ និងការរក្សាទុកវានៅក្នុងទីតាំងផ្សេងគ្នា។ ការគ្រប់គ្រងការភ្ជាប់បណ្តាញតាមរយៈModem ប្រសិនបើវាពិបាកក្នុងការគ្រប់គ្រង។

- អង្គភាពមានជម្រើសដោយបដិសេធមិនប្រើប្រាស់សេវាកម្ម និងណែនាំនិយោជិតឱ្យប្រើប្រាស់សេវាកម្មតាមរយៈ ISP ក្នុងអំឡុងពេលមានការផ្ទុះឡើងនៃមេរោគខ្លាំង អង្គភាពអាចជ្រើសរើសផ្អាកការប្រើប្រាស់កុំព្យូទ័រដែលមិនបានដំឡើងកម្មវិធីកំចាត់មេរោគជាដើម។

3.3 ផែនកំណត់ហានិភ័យ(Risk Limitation) គឺបង្កើតប្រព័ន្ធគ្រប់គ្រង ដើម្បីកាត់បន្ថយផលប៉ះពាល់នៃការគំរាមកំហែងដល់ប្រព័ន្ធ។

3.4 ផែនការហានិភ័យ(Risk planning) គឺដើម្បីគ្រប់គ្រងហានិភ័យ ដោយបង្កើតផែនការកាត់បន្ថយហានិភ័យដែលមានអាទិភាព ប្រើប្រាស់ និងថែទាំវិធីសាស្ត្រត្រួតពិនិត្យ។

3.5 ការស្រាវជ្រាវ និងការយល់ដឹងហានិភ័យ(Research and Acknowledgement) គឺដើម្បីកាត់បន្ថយការបាត់បង់ដែលបង្កឡើងដោយហានិភ័យដោយការស៊ើបអង្កេតលើភាពងាយរងគ្រោះនៃប្រព័ន្ធ និងស្រាវជ្រាវវិធីសាស្ត្រនៃការគ្រប់គ្រងដើម្បីពង្រឹងសុវត្ថិភាពរបស់ប្រព័ន្ធ។

3.6 ការផ្ទេរហានិភ័យ(Risk Transference)គឺជាការផ្ទេរហានិភ័យដោយការស្វែងរកជម្រើសដើម្បីទូទាត់សងសម្រាប់ការខាតបង់ដូចជា ឧបករណ៍បណ្តាញដែលបានទិញម្តងមានរយៈពេលធានាត្រឹមតែមួយឆ្នាំប៉ុណ្ណោះ។ ដើម្បីដោះស្រាយក្នុងករណីដែលឧបករណ៍បណ្តាញមិនដំណើរការ អង្គភាពអាចជ្រើសរើសទិញធានា៉រ៉ាប់រង ឬកិច្ចសន្យាថែទាំក្រោយពេលលក់ (Maintenance service)ជាដើម

4. ការគ្រប់គ្រងហានិភ័យ(Risk control)

- នៅពេលដែលការត្រួតពិនិត្យកើតឡើង ចាំបាច់ត្រូវកំណត់អត្តសញ្ញាណហានិភ័យធំបំផុតដែលអាចកើតមាន។ បន្ទាប់មកព្យាយាមរកវិធីកាត់បន្ថយហានិភ័យក្នុងវិធីដែលមានតម្លៃទាបដែលប៉ះពាល់ដល់បេសកកម្មផ្សេងទៀតរបស់អង្គភាពឱ្យតិចបំផុតតាមដែលអាចធ្វើទៅបាន។ ដំណើរការកាត់បន្ថយហានិភ័យអាចត្រូវបានសង្ខេបដូចខាងក្រោម។

- 1. ផ្តល់អាទិភាពដល់ការអនុវត្ត(Prioritize Actions) ពីលទ្ធផលនៃការវាយតម្លៃហានិភ័យក្នុងដំណើរការវាយតម្លៃហានិភ័យ ឈានទៅដល់លំដាប់នៃសកម្មភាពផងដែរ។ នៅក្រោមធនធានដែលមាន ជាដំបូង និងសំខាន់បំផុតគួរតែត្រូវដោះស្រាយជាមួយនឹងហានិភ័យដែលមានហានិភ័យខ្ពស់។ ដែលទាមទារឱ្យមានការជួសជុលជាបន្ទាន់ដើម្បីការពារបេសកកម្មរបស់អង្គភាព។ លទ្ធផលចុងក្រោយគឺជាលំដាប់សកម្មភាពដើម្បីគ្រប់គ្រងហានិភ័យ។

- 2.វាយតម្លៃជម្រើសត្រួតពិនិត្យ

  (Evaluate recommended Control Options) វិធីសាស្ត្រត្រួតពិនិត្យដែលបានស្នើឡើងក្នុងដំណើរការវាយតម្លៃហានិភ័យអាចមិនមែនជាជម្រើសសមស្របបំផុត ឬជាជម្រើសដែលអាចសម្រេចបានបំផុតសម្រាប់អង្គភាពនីមួយៗ។ ដូច្នេះដំហាននេះជាវិធីសាស្ត្រដែលទំនងបំផុតដែលអាចកាត់បន្ថយហានិភ័យ។ លទ្ធផលគឺជាបញ្ជីនៃវិធីសាស្ត្រត្រួតពិនិត្យ។

- 3. វិភាគអត្ថប្រយោជន៍ដែលទទួលបាន

  (Conduct Cost-Benefit Analysis) ការវិភាគអត្ថប្រយោជន៍នេះអនុញ្ញាតឱ្យផ្នែកគ្រប់គ្រងធ្វើការសម្រេចចិត្តប្រកបដោយការយល់ដឹង និងជ្រើសរើសការគ្រប់គ្រងប្រកបដោយប្រសិទ្ធភាព។

- 4.ជ្រើសរើសវិធីសាស្ត្រត្រួតពិនិត្យ (Select Control) ផ្អែកលើលទ្ធផលដែលទទួលបានពីការវិភាគអត្ថប្រយោជន៍ អ្នកគ្រប់គ្រងអាចពិនិត្យមើលវិធីសាស្ត្រត្រួតពិនិត្យទាំងអស់ ហើយជ្រើសរើសវិធីសាស្ត្រគ្របដណ្តប់។ វាគ្របដណ្តប់ទាំងការគ្រប់គ្រងបច្ចេកទេស និងប្រតិបត្តិការ រដ្ឋបាលដើម្បីធានាឱ្យបានគ្រប់គ្រាន់សម្រាប់តម្រូវការសុវត្ថិភាពនៃប្រព័ន្ធ និងអង្គភាព។
- 5.ការចាត់តាំងទំនួលខុសត្រូវ(Assign Responsibility) គឺជ្រើសរើសមនុស្សត្រឹមត្រូវដែលមានជំនាញដើម្បីគ្រប់គ្រង ត្រៀមផ្ទេរភារកិច្ច។
- 6. បង្កើតផែនការសកម្មភាពសម្រាប់បង្ការ។ (Develop a Safeguard Implementation Plan)

ប្រភេទការគ្រប់គ្រង(Control Category)

- 1. ការត្រួតពិនិត្យសុវត្ថិភាពបច្ចេកទេស(Technical Security Controls)ការគ្រប់គ្រងនេះគឺដើម្បីការពារប្រឆាំងនឹងការគំរាមកំហែងដែលអាចកើតមាន ។ ការគ្រប់គ្រងអាចត្រូវបានរាប់ពីវិធីសាស្ត្រសាមញ្ញ ទៅវិធីស្មុគស្មាញ ហើយជាធម្មតាការត្រួតពិនិត្យនេះគឺពាក់ព័ន្ធ ។ រចនាសម្ព័ន្ធស្ថាបត្យកម្មប្រព័ន្ធ វិន័យនៃវិស្វកម្ម និងសុវត្ថិភាពជារួមនៃ hardware, software និង firmware devices ដូចជា

- 1.1 គាំទ្រការគ្រប់គ្រង(Support)ទាំងនេះគឺជាការត្រួតពិនិត្យទូទៅសម្រាប់សុវត្ថិភាពនៃប្រព័ន្ធព័ត៌មានវិទ្យា រួមទាំង៖
  - ការចង្អុលបង្ហាញ(Identification)
  - ការគ្រប់គ្រងដោយប្រើសោគ្រីប(Cryptographic Key)
  - រដ្ឋបាលសន្តិសុខ(security Administration)
  - ការការពារប្រព័ន្ធ(System Protections)

- 1.2 ការគ្រប់គ្រងការពារ(Prevent) នេះគឺជាការគ្រប់គ្រងដែលការពារប្រឆាំងនឹងភាពងាយរងគ្រោះដែលកើតឡើងពីកន្លែងដែលអសន្តិសុខដំបូងបានកើតឡើង។ សម្រាប់ការត្រួតពិនិត្យបច្ចេកទេសរួមទាំង
  - ការផ្ទៀងផ្ទាត់ឈ្មោះអ្នកប្រើប្រាស់ និងពាក្យសម្ងាត់(Authentication)
  - ការផ្ទៀងផ្ទាត់អាជ្ញាប័ណ្ណ(Authorization)
  - ការពង្រឹងការគ្រប់គ្រងការចូលប្រើ(Access Control Enforcement)
  - ការបដិសេធមិនធ្វើការ (repudiation)
  - ការទំនាក់ទំនងការពារ(Protected communication) ដោយប្រើវិធីសាស្ត្រអ៊ិនគ្រីបទិន្នន័យ និងការប្រើប្រាស់បច្ចេកវិទ្យាអ៊ិនគ្រីប
  - ការរក្សាភាពឯកជនទាក់ទងនឹងធាតុទិន្នន័យដែលបានផ្លាស់ប្តូរ (Transaction Privacy)

- 1.3 ការរកឃើញ និងការគ្រប់គ្រងការស្តារឡើងវិញ(Detect and Recover) នេះជាការគ្រប់គ្រងដើម្បីរកឃើញភាពងាយរងគ្រោះក្នុងប្រព័ន្ធនិងការសង្គ្រោះទិន្នន័យ។

  វិធីសាស្ត្រត្រួតពិនិត្យរួមមាន

  - សវនកម្មប្រព័ន្ធ (Audit)
  - ការរកឃើញការឈ្លានពានប្រព័ន្ធ(Intrusion Detection)
  - ភស្តុតាងប្រព័ន្ធរួមបញ្ចូលគ្នា(Proof of wholeness)ដើម្បីវិភាគភាពត្រឹមត្រូវនៃប្រព័ន្ធ
  - ការស្តារប្រព័ន្ធទៅស្ថានភាពសុវត្ថិភាព(Restore Secure State)
  - ការរកឃើញនិងកម្ចាត់មេរោគ(Virus detection and eradication)

- 2. ការគ្រប់គ្រងសន្តិសុខរដ្ឋបាល(Management Security Controls)
  - វាគឺជាប្រតិបត្តិការមួយដើម្បីគ្រប់គ្រង និងកាត់បន្ថយការបាត់បង់ដែលបណ្តាលមកពីហានិភ័យ។ ការគ្រប់គ្រងលើការគ្រប់គ្រងផ្តោតលើតម្រូវការនៃគោលការណ៍ការពារទិន្នន័យសាជីវកម្ម និងស្តង់ដារនាំឱ្យមានដំណើរការប្រតិបត្តិការដែលឆ្លើយតបទៅនឹងគោលដៅ និងបេសកកម្មរបស់អង្គភាព។

- 3. ការត្រួតពិនិត្យសុវត្ថិភាពប្រតិបត្តិការ(Operational Security Controls)ស្តង់ដារសុវត្ថិភាពរបស់អង្គការគួរតែរួមបញ្ចូលសំណុំនៃការត្រួតពិនិត្យ និងការណែនាំ ដើម្បីធានាថាដំណើរការសុវត្ថិភាពត្រូវបានអនុវត្តយ៉ាងត្រឹមត្រូវ។ របៀបគ្រប់គ្រងវាក្នុងការអនុវត្ត ពាក់ព័ន្ធនឹងការបំបាត់កំហុសមុខងារគំរាមកំហែងកំពុងកើតឡើង។ អាចបែងចែកជាពីរក្រុមដូចខាងក្រោម:

❖3.1 ការត្រួតពិនិត្យសុវត្ថិភាពសិក្ខាសាលាបង្ការ

(Preventive Operational Controls) ឧទាហរណ៍

3.1.1 ការត្រួតពិនិត្យសុវត្ថិភាពសិក្ខាសាលាបង្ការ

3.1.2 ការចែកចាយព័ត៌មានខាងក្រៅមានកំណត់

3.1.3 គ្រប់គ្រងមេរោគកម្មវិធី

3.1.4 ការគ្រប់គ្រងទ្រព្យសម្បត្តិព័ត៌មាន ដើម្បីការពារ
ការខូចខាតភ្លើង

❖3.2 ការត្រួតពិនិត្យសុវត្ថិភាពសិក្ខាសាលាបង្ការ

(Preventive Operational Controls) ឧទាហរណ៍

3.2.1 ការប្រើប្រាស់វិធីសាស្ត្រសុវត្ថិភាពរូបវន្ត ដូចជាការប្រើប្រាស់ទូរទស្សន៍បិទជិត ការដំឡើងឧបករណ៍ចាប់សញ្ញាជាដើម។

3.2.2 រក្សាសុវត្ថិភាពក្នុងបរិស្ថាន ដូចជាការប្រើឧបករណ៍ចាប់សញ្ញាជាដើម។

5. របាយការណ៍ហានិភ័យសំណល់(Residual risk reporting)

- នៅពេលដែលហានិភ័យត្រូវបានកាត់បន្ថយ ចាំបាច់ត្រូវរាយការណ៍ និងពិនិត្យឱ្យបានទៀងទាត់ ដើម្បីមើលថាតើវាត្រូវបានវាយតម្លៃដែរឬទេ និងការវាយតម្លៃហានិភ័យគ្រប់ពេលវេលា ហើយមើលថាតើវិធានការត្រួតពិនិត្យផ្សេងៗមានប្រសិទ្ធភាពឬអត់ វិធីសាស្ត្រស្តង់ដារដែលប្រើជាទូទៅគឺដើម្បីឱ្យមានអង្គភាពខាងក្នុង ឬខាងក្រៅដែលត្រូវបានធ្វើសវនកម្មដោយដំណើរការសវនកម្ម IT ដែលសមស្រប ដោយសារបរិយាកាសនិងបទប្បញ្ញត្តិមានភាពច្បាស់លាស់ និងផ្លាស់ប្តូរគ្រប់ពេលវេលា។ ដូច្នេះការគ្រប់គ្រងហានិភ័យ និងសវនកម្មទៀងទាត់ត្រូវបានទាមទារ។

6. ការត្រួតពិនិត្យ(Monitoring)

- ដំណើរការត្រួតពិនិត្យធានាថា អង្គការមានវិធានការផ្សេងៗចាំបាច់និងសមរម្យសម្រាប់ ការគ្រប់គ្រងហានិភ័យផ្សេងៗ ហើយវិធានការទាំងនោះត្រូវបានអនុវត្តតាមនិងមានលទ្ធផលពិតប្រាកដ។

Assigment

- What is information security (IS) and risk management? And what are information risks?
- What are the key steps of a risk management process ?

End of Chapter

Thank You