សម្រាប់សហគ្រាសខ្នាតតូចនិងមធ្យម (SMEs) និងប្រតិបត្តិករអាជីវកម្មខ្នាតតូច

ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើសន្តិសុខព័ត៌មានរយៈពេល 5-នាទី

តើអ្នកដើរទាន់និន្នាការចុងក្រោយបំផុតដែរឬទេ?

ការផ្លាស់ប្តូរនានាក្នុងការគំរាមកំហែងនិងការវាយប្រហារ

- កម្មវិធីមេរោគចាប់ជំរិត (Ransomware)
- ការវាយប្រហារបញ្ជីលេខកូដសម្ងាត់
- ការវាយប្រហារអ៊ីម៉ែលគោលដៅ

ការផ្លាស់ប្តូរនានាក្នុងមជ្ឈដ្ឋានព័ត៌មានវិទ្យា (IT)

- បច្ចេកវិទ្យាក្លាវដ៍ (Cloud)
- ថែបផ្លឺត
- ទូរស័ព្ទស្មាតហ្វូន

ប្រើប្រាស់ **"តារាងស្វ័យវាយតម្លៃក្រុមហ៊ុនរយៈពេល ៥នាទី"** ដើម្បីត្រួតពិនិត្យលក្ខណៈនៃស្ថានភាពសន្តិសុខក្រុមហ៊ុនរបស់អ្នកនៅមុនពេលដែលអ្នកបាត់បង់ទិន្នន័យណាមួយ!

ASEAN · JAPAN
Cybersecurity Cooperation

ស្វ័យវាយតម្លៃ

១ សូមអានវាមុនពេលធ្វើការវាយតម្លៃ។

របៀបប្រើ

យើងបានផ្តោតជាសំខាន់លើវិធានការសន្តិសុខព័ត៌មានចំនួន ២៥ ដែលមានប្រសិទ្ធភាព និងអាចអនុវត្តបាននៅក្នុងកម្រិតនៃការចំណាយទាបសម្រាប់ស្ថាប័ន។
សូមត្រួតពិនិត្យស្ថានភាពអនុវត្តនៃចំណុចទាំងអស់នេះ និងអនុវត្តវិធានការណាមួយដែលពុំទាន់បានអនុវត្ត នៅពេលអានសេចក្តីពន្យល់នៅក្នុងកូនសៀវភៅផ្សព្វផ្សាយនេះ។

គោលបំណង និងអត្ថប្រយោជន៍

- វាអាចឲ្យអ្នកយល់ដឹងអំពីបញ្ហាណាមួយដែលអាចកើតមានឡើង។
- ដោយយល់ដឹងពីបញ្ហាទាំងអស់នេះ អ្នកអាចស្វែងរកវិធានការជាក់លាក់ដើម្បីអនុវត្តនៅជំហានបន្ទាប់ទៀត។

របៀបអានសេចក្តីពណ៌នា

សូមធ្វើការវិនិច្ឆ័យដោយពុំពឹងផ្អែកលើឧទាហរណ៍ជាក់លាក់នៅក្នុងខ្លឹមសារនៃសេចក្តីពិពណ៌នានេះ។ ឧទាហរណ៍ ខ្លឹមសារនៃសំណួរទី១៦ គឺនិយាយអំពី “វិធានការបង្ការអំពើចោរកម្ម"។ វិធានការនេះសួរថាតើអ្នកអនុវត្តជំហាននានាដើម្បីបង្ការអំពើចោរកម្មដោយដាក់កុំព្យូទ័រយួរដៃនៅក្នុងថតទូដែរឬទេ ប្រសិនបើស្ថាប័នរបស់អ្នកប្រើកុំព្យូទ័រយួរដៃ។
វិធានការនេះក៏សាកសួរផងដែរថាតើអ្នកអនុវត្តជំហាននានាដើម្បីបង្ការអំពើចោរកម្ម ដោយមិនទុកគ្រឿងបរិក្ខារអេឡិចត្រូនិកដូចជា USB drive ឬហាដឌីសខាងក្រៅ (external hard drives) នៅលើតុដែរឬទេ ប្រសិនបើស្ថាប័នរបស់អ្នកមិនប្រើប្រាស់កុំព្យូទ័រយួរដៃទេនោះ។
សូមអានកូនសៀវភៅផ្សព្វផ្សាយនេះ ប្រសិនបើអ្នកមិនយល់អំពីគោលបំណងនៃសំណួរណាមួយ ឬប្រសិនបើអ្នកគិតថាវាពិបាកយល់។

ប្រសិនបើក្រុមហ៊ុនរបស់អ្នក ពុំបានប្រើប្រាស់ចំណុចណាមួយទេនោះ

ចំណុចមួយចំនួនខាងក្រោម អាចមិនអនុវត្តចំពោះក្រុមហ៊ុនរបស់អ្នកនោះទេ អាស្រ័យលើប្រភេទនៃអាជីវកម្ម។ នៅក្នុងករណីទាំងអស់នោះ សូមគូសរង្វង់ជុំវិញពាក្យ “បានអនុវត្តរួច”។

- លេខ ៤ ម៉ាស៊ីនថតចម្លងភ្ជាប់ទៅនឹងខ្សែបណ្តាញ និងហាដឌីស (hard drives)
- លេខ ៥ សេវាគេហទំព័រ
- លេខ ៩ បណ្តាញឥតខ្សែ (Wireless LANs)
- លេខ ២៣ សេវាបច្ចេកវិទ្យាក្លាវដ៍ (Cloud services)

ប្រសិនបើអ្នកគិតថា យើងពុំមាន ‘ព័ត៌មានសម្ងាត់’ ណាមួយទេនោះ ចំណុចខាងក្រោមនេះ ត្រូវចាត់ទុកជាព័ត៌មានសម្ងាត់!

- អាសយដ្ឋានរបស់និយោជិត និងបញ្ជីបើកប្រាក់បៀវត្ស
- បញ្ជីបង់ប្រាក់សម្រាប់ដៃគូអាជីវកម្មនីមួយៗ និងព័ត៌មានប្រតិបត្តិការសាច់ប្រាក់
- ព័ត៌មានគណនេយ្យស្ថាប័នរបស់អ្នក
- បញ្ជីព័ត៌មានសម្រាប់ទំនាក់ទំនងអតិថិជន និងដៃគូអាជីវកម្ម
- ការបង្កើតព័ត៌មានដូចជា គំនូរចនា (design drawing) សម្រាប់ផលិតផលថ្មី
- ព័ត៌មានណាមួយពីដៃគូអាជីវកម្មដែលគប្បីត្រូវធ្វើការគ្រប់គ្រងដោយប្រុងប្រយ័ត្ន

មានព័ត៌មានខ្លះដែលត្រូវចាត់ចែងទុកជាព័ត៌មានសម្ងាត់ក្នុងចំណោមព័ត៌មានសំខាន់ៗផ្សេងទៀតរបស់ស្ថាប័ន។ អ្នកត្រូវធ្វើការបញ្ជាក់ និងរៀបចំថាតើប្រភេទនៃព័ត៌មានអ្វីខ្លះដែលមាននៅក្នុងក្រុមហ៊ុនរបស់អ្នក ដែលត្រូវចាត់ទុកជាព័ត៌មានសម្ងាត់។ ការធ្វើចំណាត់ថ្នាក់ទិន្នន័យ គឺជាជំហានដំបូងនៃសន្តិសុខព័ត៌មាន។

២ សូមឆ្លើយសំណួរទាំង ២៥ នៅក្នុងតារាងស្វ័យវាយតម្លៃក្រុមហ៊ុន

ប្រសិនបើអ្នកបានពិន្ទុគ្រប់ ១០០	វិធានការសន្តិសុខមូលដ្ឋានរបស់អ្នក គឺបានល្អឥតខ្ចោះហើយ។ គិតអំពីការអនុវត្តវិធានការរបស់អ្នកដើម្បីបន្តទៅកាន់កម្រិតបន្ទាប់ទៀត។
ប្រសិនបើអ្នកបានពិន្ទុពី ៧០-៩៩	ជិតបានល្អឥតខ្ចោះហើយ ប៉ុន្តែនៅមានផ្នែកខ្លះទៀតដែលមិនទាន់មានវិធានការពេញលេញនៅឡើយ។
ប្រសិនបើអ្នកបានពិន្ទុពី ៥០-៦៩	មានកន្លែងងាយមើលឃើញមួយចំនួនដែលមានវិធានការមិនទាន់ពេញលេញនៅឡើយ។
ប្រសិនបើអ្នកបានពិន្ទុពី ៤៩ ឬតិចជាងនេះ	នោះគ្មានអ្វីចម្លែកទេ ប្រសិនបើមានករណីដូចជាការបែកធ្លាយទិន្នន័យកើតមានឡើង។

វិធានការដែលរៀបរាប់នៅក្នុងតារាងស្វ័យវាយតម្លៃក្រុមហ៊ុន ត្រូវបានកំណត់ដូចខាងក្រោម។

- ■ ផ្នែកប្រតិបត្តិ (អ្នកតំណាង) អាចធ្វើការណែនាំដោយផ្ទាល់ និងធ្វើការបញ្ជាក់ថាតើវិធានការគោលនយោបាយ ត្រូវបានគេអនុវត្តដែរឬទេ។
- ■ គ្រប់និយោជិតទាំងអស់ ត្រូវទទួលស្គាល់គ្នាទៅវិញទៅមក។
- ■ ក្រុមហ៊ុនពុំមានម៉ាស៊ីនមេ (server) ឬ ឧបករណ៍បណ្តាញផ្ទាល់ខ្លួន ដែលតម្រូវឲ្យមានការដំឡើងសាំញ៉ាំនៅឯក្រុមហ៊ុននោះទេ។
  - • វេបសាយ របស់ក្រុមហ៊ុន ពុំប្រើប្រាស់ប្រើប្រាស់ម៉ាស៊ីនមេ (server) ដែលភ្ជាប់ដោយផ្ទាល់ទៅនឹងអ៊ីនធឺណិត ដូចជាសេវាបច្ចេកវិទ្យាក្លាវដ៍ជាដើម។
  - • ពុំមានសូហ្វវែរកម្មវិធីដែលបានបង្កើតឡើងដោយក្រុមហ៊ុននោះទេ ហើយក្រុមហ៊ុនប្រើតែសូហ្វវែរកម្មវិធីដែលមានលក់ជាលក្ខណៈអាជីវកម្មតែប៉ុណ្ណោះ។
  - • កុំព្យូទ័រផ្ទាល់ខ្លួន ត្រូវបានអនុញ្ញាតឲ្យប្រើសម្រាប់ធ្វើការតែក្នុងករណីដែលកុំព្យូទ័រនោះស្ថិតក្រោមលក្ខខណ្ឌនៃការអនុវត្តវិធានការដូចគ្នានឹងកុំព្យូទ័រគ្រប់គ្រងដោយក្រុមហ៊ុនតែប៉ុណ្ណោះ។

ស្វ័យវាយតម្លៃ

តារាងស្វ័យវាយតម្លៃក្រុមហ៊ុនរយៈពេល ៥នាទី

តារាងស្វ័យវាយតម្លៃក្រុមហ៊ុន កំណត់វិធានការសន្តិសុខព័ត៌មានដែលអ្នកគប្បីត្រូវចាត់ទុកជាចំណុចអាទិភាពក្នុងនាមជាស្ថាប័នមួយ។

- សូមអានចំណុច ① នៅទំព័រខាងដើមមុនពេលធ្វើការវាយតម្លៃនេះ។
- សូមអានចំណុចវាយតម្លៃខាងក្រោម និងគូសរង្វង់ក្នុងចន្លោះដែលត្រឹមត្រូវ។
- តារាងនេះ ត្រូវបំពេញដោយផ្នែកប្រតិបត្តិ ឬអ្នកគ្រប់គ្រង។
- សូមឆ្លើយសំណួរថាតើចំណុចនានាដែលបង្ហាញដោយសញ្ញា 👤 ត្រូវបានអនុវត្តដោយនិយោជិតគ្រប់រូបដែរឬទេ។ ប្រសិនបើចំណុចណាមួយ ត្រូវបានអនុវត្តដោយនិយោជិតមួយចំនួនតែប៉ុណ្ណោះ សូមជ្រើសរើស “បានអនុវត្តដោយផ្នែក”។
- សូមឆ្លើយសំណួរថាតើចំណុចនានាដែលបង្ហាញដោយសញ្ញា 🏢 ត្រូវបានអនុវត្តដោយក្រុមហ៊ុនរបស់អ្នកដែរឬទេ។
- បូកពិន្ទុរបស់អ្នកនៅផ្នែកខាងក្រោមនៃទំព័រនេះ ហើយបន្តអានចំណុច ② នៅទំព័រខាងដើម។

ស្ថាប័ន៖

អ្នកឆ្លើយតប៖

កាលបរិច្ឆេទ៖

ចំណុចវាយតម្លៃ	ល.រ.	ពិពណ៌នា	ចម្លើយតប			
			បានអនុវត្ត	បានអនុវត្តដោយផ្នែក	មិនបានអនុវត្ត	មិនដឹង
ផ្នែកទី ១ វិធានការមូលដ្ឋាន	១	👤 តើអ្នកបានធ្វើការអាប់ដេតប្រព័ន្ធប្រតិបត្តិការ (OS) ឬសូហ្វវែររបស់អ្នកដែរឬទេ? *1 ឬប្រើប្រាស់វិធានការដទៃផ្សេងទៀតដែរឬទេ?	៤	២	0	0
	២	👤 តើអ្នកបានចាត់វិធានការដើម្បីការពារកុំព្យូទ័រ (PC) របស់អ្នកពីមេរោគផ្សេងៗ ដូចជាការដំឡើងសូហ្វវែរកម្ចាត់មេរោគ ធ្វើការអាប់ដេតដោយស្វ័យប្រវត្តិដែរឬទេ?*2	៤	២	0	0
	៣	👤 តើអ្នកបានកំណត់លេខកូដសម្ងាត់រឹងមាំ ដែលមិនងាយស្រួលនឹងទាយដឹង និងមិនប្រើប្រាស់លេខកូដសម្ងាត់ដូចជាឈ្មោះ លេខទូរស័ព្ទ ឬថ្ងៃខែឆ្នាំរបស់អ្នក ហើយតើអ្នកបានជៀសវៀងពីការប្រើប្រាស់លេខកូដសម្ងាត់ដូចគ្នាសម្រាប់សេវាអនឡាញ ដែលអ្នកប្រើប្រាស់ ជាច្រើននោះដែរឬទេ?	៤	២	0	0
	៤	👤 តើអ្នកបានរឹតបន្តឹងចំពោះការចូលទៅប្រើប្រាស់ព័ត៌មានសម្ងាត់បានត្រឹមត្រូវដែរឬទេ ដូចជាការកំណត់លើការចែករំលែកម៉ាស៊ីនថតចម្លងដែលភ្ជាប់ទៅនឹងបណ្តាញ ឬហាដឌីស (hard drives) សម្រាប់តែអ្នកដែលត្រូវការប្រើវាតែប៉ុណ្ណោះដែរឬទេ?	៤	២	0	0
	៥	👤🏢 តើអ្នកមានប្រព័ន្ធមួយដែលកំពុងដាក់ដំណើរការដើម្បីកំណត់ពីការគំរាមកំហែងនិងវិធីសាស្ត្រវាយប្រហារថ្មីៗ និងចែករំលែកវាសម្រាប់ប្រើប្រាស់ផ្ទៃក្នុងដោយធ្វើការត្រួតពិនិត្យ និងចែករំលែកការព្រមានពីក្រុមហ៊ុនផលិត ឬវេបសាយ *៣ ដែលអ្នកប្រើប្រាស់ដែរឬទេ?	៤	២	0	0
ផ្នែកទី ២ វិធានការក្នុងនាមជានិយោជិត	៦	👤 តើអ្នកមានការប្រុងប្រយ័ត្នចំពោះអ៊ីម៉ែលបោកបញ្ឆោត (phishing e-mails) និងព្យាយាមមិនបើកឯកសារភ្ជាប់នៅក្នុងសារដែលមានការសង្ស័យ ឬចុចលើតំណភ្ជាប់នៅក្នុងសារនោះដែរឬទេ?	៤	២	0	0
	៧	👤 តើអ្នកមានប្រព័ន្ធដែលកំពុងដាក់ឲ្យដំណើរការដើម្បីត្រួតពិនិត្យ និងការពារការផ្ញើអ៊ីម៉ែលខុស ដូចជាការត្រួតពិនិត្យឡើងវិញលើអាសយដ្ឋាននៅមុនពេលផ្ញើអ៊ីម៉ែលដែរ ឬទេ?	៤	២	0	0
	៨	👤 តើអ្នកការពារព័ត៌មានសំខាន់ដោយការពារឯកសារភ្ជាប់ដោយប្រើលេខកូដសម្ងាត់ ឬវិធានការដទៃផ្សេងទៀតស្រដៀងគ្នានេះ នៅមុនពេលធ្វើឯកសារទៅក្រៅតាមអ៊ីម៉ែលដែរឬទេ?	៤	២	0	0
	៩	👤 តើអ្នកបានចាត់វិធានការនានាដើម្បីរក្សាសន្តិសុខបណ្តាញឥតខ្សែ (wireless LANs) របស់អ្នក ដូចជាការអនុវត្តការ ធ្វើកូដនីយកម្ម (encryption) នៅពេលប្រើវាដែរឬទេ?	៤	២	0	0
	១០	👤 តើអ្នកបានអនុវត្តជំហាននានាដើម្បីគ្រប់គ្រងការប្រើប្រាស់អ៊ីនធឺណិត ដូចជាវិធានកំណត់ចំពោះការស្វែងរកនៅលើវេបសាយ និងការបង្ហោះអ្វីផ្សេងៗនៅលើបណ្តាញព័ត៌មានសង្គមដោយប្រើកុំព្យូទ័រការិយាល័យដែរឬទេ?	៤	២	0	0
	១១	👤 តើអ្នកបានអនុវត្តជំហាននានាដើម្បីធ្វើការរក្សាទុកទិន្នន័យបម្រុង (backups) ជាទៀងទាត់ដែរឬទេ ដើម្បីការពារព័ត៌មានសំខាន់ពីការបាត់បង់ដោយសារដំណើរការខុសប្រក្រតី ឬកំហុសផ្នែកប្រតិបត្តិការដែរឬទេ?	៤	២	0	0
	១២	👤 តើអ្នកបានអនុវត្តជំហាននានាដើម្បីការពារការបាត់បង់ ឬការលេចធ្លាយព័ត៌មានសំខាន់ ដូចជាការរក្សាទុកព័ត៌មានសំខាន់នៅក្នុងទូរចាក់សោជាដងទុករានៅលើតុដែរឬទេ?	៤	២	0	0
	១៣	👤 នៅពេលយកព័ត៌មានសំខាន់ចេញក្រៅការិយាល័យ តើអ្នកបានអនុវត្តជំហាននានាប្រឆាំងនឹងអំពើចោរកម្ម ឬការបាត់បង់ ដូចជាការការពារព័ត៌មានទាំងនោះដោយប្រើលេខកូដសម្ងាត់ ឬការបម្លែងកូដ និងការរក្សាទុកវាជាមួយអ្នកនៅគ្រប់វេលាទាំងអស់ដែរឬទេ?	៤	២	0	0
	១៤	👤 តើអ្នកបានអនុវត្តវិធាននានាដើម្បីធានាថាអ្នកដទៃមិនអាចប្រើប្រាស់កុំព្យូទ័ររបស់អ្នកបាន ដូចជាការកំណត់ការចាក់សោនៅលើឆ្នាំងកុំព្យូទ័រនៅពេលអ្នកចាកចេញពីតុធ្វើការរបស់អ្នកដែរឬទេ?	៤	២	0	0
	១៥	👤 តើអ្នកព្យាយាមការពារមនុស្សដែលគ្មានការអនុញ្ញាតមិនឲ្យចូលទៅក្នុងការិយាល័យដោយទៅជិតមនុស្សចម្លែកនៅពេលអ្នកកត់សម្គាល់មនុស្សណាម្នាក់ដែលមិនធ្លាប់ស្គាល់នៅការិយាល័យ ឬតាមរយៈការចាត់វិធានការណាមួយផ្សេងទៀតដែរឬទេ?	៤	២	0	0
	១៦	👤 តើអ្នកបានអនុវត្តជំហាននានាដើម្បីការពារអំពើចោរកម្មនៅពេលចាកចេញពីការិយាល័យនៅពេលថ្ងៃ ដូចជាការចាក់សោកុំព្យូទ័រយួរដៃ និងបរិក្ខារផ្សេងៗនៅក្នុងថតតុ ជាជាងទុកវាចោលនៅលើតុការងារដែរឬទេ?	៤	២	0	0
	១៧	👤 តើកូនសោការិយាល័យត្រូវបានគ្រប់គ្រងត្រឹមត្រូវដែរឬទេ ដូចជាមនុស្សដែលចាកចេញពីការិយាល័យក្រោយគេត្រូវចាក់សោការិយាល័យ និងធ្វើការកត់ត្រា (ឈ្មោះរបស់ពួកគេ កាលបរិច្ឆេទ និងពេលវេលា) ដែរឬទេ?	៤	២	0	0
	១៨	👤 នៅពេលបោះចោលព័ត៌មានសំខាន់ៗ តើអ្នកអនុវត្តជំហាននានាដើម្បីធ្វើយ៉ាងណាឲ្យព័ត៌មានសំខាន់នោះមិនអាចអានបាន ដូចជាការកាត់ឯកសារជាកម្មេចតូចៗ ឬប្រើប្រាស់កម្ទេវិធីលុបទិន្នន័យដែរឬទេ?	៤	២	0	0
ផ្នែកទី ៣ វិធានការក្នុងនាមជាស្ថាប័ន	១៩	🏢 តើអ្នកមានក្រមប្រតិបត្តិសម្រាប់និយោជិតដើម្បីរក្សាព័ត៌មានសម្ងាត់ ដូចជាការជូនដំណឹងដល់និយោជិតនៅពេលជ្រើសរើសពួកគេឲ្យបម្រើការងារ ដែលពួកគេត្រូវមានកាតព្វកិច្ចក្នុងការរក្សាព័ត៌មានសម្ងាត់ និងអំពីលក្ខខណ្ឌមួយចំនួនសម្រាប់ការពិន័យដែរឬទេ?	៤	២	0	0
	២០	🏢 តើអ្នកអនុវត្តការបណ្តុះបណ្តាលលើកកម្ពស់ការយល់ដឹងដើម្បីឲ្យនិយោជិតមានការយល់ដឹងអំពីសារៈសំខាន់នៃការគ្រប់គ្រងព័ត៌មាន ដូចជាការពន្យល់ជាប្រចាំអំពីសារៈសំខាន់នៃការគ្រប់គ្រងព័ត៌មានដែរឬទេ?	៤	២	0	0
	២១	🏢 តើអ្នកបានបញ្ជាក់ច្បាស់ថាតើនិយោជិតអាចប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកផ្ទាល់ខ្លួននៅក្នុងការងាររបស់ពួកគេបានដែរឬទេ ដូចជាការកំណត់គោលនយោបាយស្តីពីការប្រើប្រាស់កុំព្យូទ័រផ្ទាល់ខ្លួននិងទូរស័ព្ទស្មាតហ្វូននៅក្នុងនិងនៅក្រៅក្រុមហ៊ុនជាដើម?	៤	២	0	0
	២២	🏢 តើអ្នកតម្រូវឲ្យដៃគូអាជីវកម្មរក្សាការសម្ងាត់ ដូចជាការរួមបញ្ចូលលក្ខខណ្ឌស្តីពីការរក្សាការសម្ងាត់ (កាតព្វកិច្ចរក្សាព័ត៌មានសម្ងាត់) នៅក្នុងកិច្ចសន្យាដែរឬទេ?	៤	២	0	0
	២៣	🏢 តើអ្នកបញ្ជាក់ច្បាស់ពីសុវត្ថិភាពនិងទំនុកចិត្តផ្នែកសេវាកម្មដោយត្រួតពិនិត្យលក្ខខណ្ឌនៃការប្រើប្រាស់ និងវិធានការសន្តិសុខនៅមុនពេលជ្រើសរើសសេវាពីខាងក្រៅ ដូចជាសេវាបច្ចេកវិទ្យាក្លាវដ៍ដែរឬទេ?	៤	២	0	0
	២៤	🏢 តើមានត្រៀមរៀបចំជាស្រេចនៅក្នុងករណីមានគ្រោះថ្នាក់ផ្នែកសន្តិសុខព័ត៌មាន ដូចជាការធ្វើសេចក្តីព្រាងអំពីនីតិវិធីក្នុងការឆ្លើយតបទៅនឹងការលេចធ្លាយ ការបាត់បង់ ឬការលួចព័ត៌មានសម្ងាត់ដែរឬទេ?	៤	២	0	0
	២៥	🏢 តើអ្នកបានកំណត់ខ្លឹមសារនៃវិធានការសន្តិសុខព័ត៌មាន ដូចជាការបង្កើតវិធានការសន្តិសុខព័ត៌មាន (ដូចជាចំណុច 1 ដល់ 24 ខាងលើ) ក្នុងលក្ខណៈជាគោលនយោបាយក្រុមហ៊ុនដែរឬទេ?	៤	២	0	0

*១ កម្មវិធីមួយដែលផ្តល់ដោយក្រុមហ៊ុន Microsoft Corporation ដែលជួយជួសជុលការខូចខាតនៅលើកុំព្យូទ័រប្រើប្រាស់កម្មវិធី Windows

*២ ឯកសារមូលដ្ឋានទិន្នន័យ (database file) ដែលហៅថា “ឯកសារទម្រង់ (pattern file)” សម្រាប់ចាប់មេរោគក្នុងកុំព្យូទ័រ

*៣ ឈ្មោះទូទៅនៃសេវាកម្មនានាដែលប្រើតាមអ៊ីនធឺណិតដូចជា សេវាធនាគារតាមអ៊ីនធឺណិត បណ្តាញព័ត៌មានសង្គម វែបម៉ែល (webmail) និងប្រតិទិនជាដើម

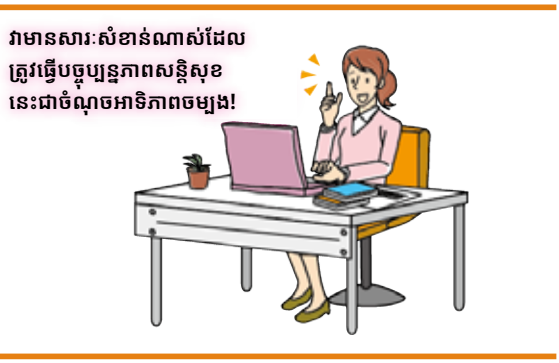
★ ពុំមានការធានាថាវិធានការដែលបានរៀបរាប់នៅក្នុងតារាងស្វ័យវាយតម្លៃក្រុមហ៊ុន ផ្តល់នូវការការពារពេញលេញទាំងស្រុងនោះទេ។

A ពិន្ទុសរុបនៃការងារដែលបានអនុវត្ត	B ពិន្ទុសរុបនៃការងារដែលបានអនុវត្តដោយផ្នែក	A+B ពិន្ទុ
ពិន្ទុ	ពិន្ទុ	ពិន្ទុ

សេចក្តីពន្យល់

ផ្នែកទី ១ វិធានការមូលដ្ឋាន

ចំណុចលេខ១ ដល់លេខ៥ គឺជាវិធានការនានាដែលគប្បីត្រូវអនុវត្ត ដោយមិនគិតអំពីទំហំ និងទម្រង់ក្រុមហ៊ុននោះទេ។ វាមានសារៈសំខាន់ដែលត្រូវធ្វើការត្រួតពិនិត្យវិធានការទាំងអស់នេះជាបន្តបន្ទាប់ ហើយមិនមែនត្រូវធ្វើតែម្តងនោះទេ។ វាពិតជាមានសារៈសំខាន់ណាស់ក្នុងការអនុវត្តវិធានការទាំងនេះក្នុងនាមជាវិធានរបស់ក្រុមហ៊ុន ដើម្បីឲ្យនិយោជិតទាំងអស់អាចអនុវត្តតាមវិធានការទាំងនេះបាន។



ចំណុចលេខ ១ តារាងលេខ១ ស្តីពីស្ថ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានការចំពោះភាពងាយរងគ្រោះ

ត្រូវធ្វើឲ្យប្រព័ន្ធប្រតិបត្តិការ (OS) និងសូហ្វវែររបស់អ្នកមានភាពទាន់សម័យ

ការមិនអើពើចំពោះបញ្ហាសន្តិសុខនៃប្រព័ន្ធប្រតិបត្តិការ (OS) និងសូហ្វវែរ ធ្វើឲ្យឧបករណ៍អេឡិចត្រូនិករបស់អ្នកមានភាពងាយរងគ្រោះទៅនឹងការឆ្លងមេរោគ។ ត្រូវប្រាកដថាបានធ្វើការអាប់ដេតប្រព័ន្ធប្រតិបត្តិការ (OS) និងសូហ្វវែររបស់អ្នក ឬប្រើប្រាស់កំណែប្រែ (version) ចុងក្រោយគេបំផុត។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការប្រើប្រាស់ Windows Update (ប្រព័ន្ធប្រតិបត្តិការប្រើកម្មវិធី Windows) ឬប្រើប្រាស់កំណែប្រែ (version) ចុងក្រោយគេបំផុតនៃកម្មវិធី Adobe Flash Player, Adobe Reader, Java និងសូហ្វវែរដទៃផ្សេងទៀត។

ចំណុចលេខ ២ តារាងលេខ២ ស្ថ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានការកម្ចាត់មេរោគ

ការដំឡើងសូហ្វវែរកម្ចាត់មេរោគ និងការប្រើប្រាស់វាឲ្យបានត្រឹមត្រូវ

មានការកើនឡើងនូវចំនួនមេរោគជាច្រើនដែលលួចយក ID និងលេខកូដសម្ងាត់ប្រតិបត្តិកុំព្យូទ័រពីចម្ងាយ និងកូដនីយកម្ម ឯកសារតាមអំពើចិត្ត។ ត្រូវប្រាកដថាបានដំឡើងសូហ្វវែរកម្ចាត់មេរោគ និងត្រូវធានាថា definition file សម្រាប់ចាប់មេរោគគឺមានភាពទំនើបទាន់សម័យជានិច្ច។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការកំណត់ឲ្យឧបករណ៍អេឡិចត្រូនិករបស់អ្នកឲ្យអាប់ដេត virus definition file ដោយស្វ័យប្រវត្តិ និងពិចារណាអំពីការដំឡើងសូហ្វវែរពង្រឹងសន្តិសុខជាដើម។

ចំណុចលេខ ៣ តារាងលេខ៣ ស្ថ័យវាយតម្លៃក្រុមហ៊ុនលើការគ្រប់គ្រងលេខកូដសម្ងាត់

ការប្រើប្រាស់លេខកូដសម្ងាត់រឹងមាំ

មានការកើនឡើងនូវចំនួននៃការខូចខាតពីការចូលទៅវេបសាយដោយពុំមានការអនុញ្ញាត ដោយសារលេខកូដសម្ងាត់ត្រូវបានទាយដឹង និងការប្រើប្រាស់ពុំបានត្រឹមត្រូវនៃ ID និងលេខកូដសម្ងាត់ដែលបានលេចធ្លាយពីសេវាអនឡាញណាមួយ។ ត្រូវប្រាកដថាលេខកូដសម្ងាត់របស់អ្នករឹងមាំដោយធ្វើឲ្យវាវែង និងមានភាពស្មុគស្មាញ ហើយមិនត្រូវប្រើប្រាស់វាសាជាថ្មីនោះទេ។

*លេខកូដសម្ងាត់ងាយៗ៖ លេខកូដសម្ងាត់មួយដែលមានភាពងាយស្រួលក្នុងការទាយដឹងបានដោយភាគីទីបីដូចជាឈ្មោះរបស់អ្នក ឈ្មោះក្រុមហ៊ុន ឬពាក្យអង់គ្លេសងាយៗនៅក្នុងវចនានុក្រម។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការធ្វើឲ្យលេខកូដសម្ងាត់មានការផ្សំបញ្ចូលគ្នានូវតួអក្សរ លេខ ឬសញ្ញាពិសេសចំនួន 10 ឬច្រើនជាងនេះ។ ហាមប្រើឈ្មោះ លេខទូរសព្ទ ថ្ងៃ-ខែ-ឆ្នាំកំណើត ។ល។ និងមិនត្រូវប្រើលេខកូដសម្ងាត់ដូចគ្នាសម្រាប់សេវាអនឡាញ និងគេហទំព័រដទៃផ្សេងទៀតឡើយ។

ចំណុចលេខ ៤ តារាងលេខ៤ ស្ថ័យវាយតម្លៃក្រុមហ៊ុនលើការកំណត់ឧបករណ៍អេឡិចត្រូនិក

ត្រួតពិនិត្យការកំណត់ការចែករំលែកព័ត៌មាន

មានការកើនឡើងនូវក្តីបារម្ភអំពីការត្រួតពិនិត្យមើលព័ត៌មានដោយមនុស្សដែលគ្មានការអនុញ្ញាត ដោយសារទិន្នន័យរក្សាទុកនៅហ្វាល់សើវើ (file servers) ឬកន្លែងរក្សាទុកទិន្នន័យតាមប្រព័ន្ធអនឡាញ ឬម៉ាស៊ីនថតចម្លងដែលភ្ជាប់ទៅបណ្តាញពុំបានត្រឹមត្រូវ។ ត្រូវប្រាកដថាម៉ាស៊ីនមេ (servers) និងឧបករណ៍ភ្ជាប់បណ្តាញ ត្រូវបានចែករំលែកជាមួយតែអ្នកណាដែលទទួលបានការអនុញ្ញាតឲ្យចូលទៅកាន់ព័ត៌មានទាំងនោះប៉ុណ្ណោះ។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាកំណត់វិសាលភាពនៃការចែករំលែកសេវាបច្ចេកវិទ្យាក្លាវដ៍ (cloud services) ការកំណត់វិសាលភាពនៃឧបករណ៍អេឡិចត្រូនិកភ្ជាប់បណ្តាញរួម និងការផ្លាស់ប្តូរការកំណត់នានា នៅពេលនិយោជិតផ្លាស់ទៅកាន់ផ្នែកបម្រើការផ្សេង ឬចូលនិវត្តន៍។

ចំណុចលេខ ៥ តារាងលេខ៥ ស្ថ័យវាយតម្លៃក្រុមហ៊ុន លើការប្រមូលព័ត៌មាន

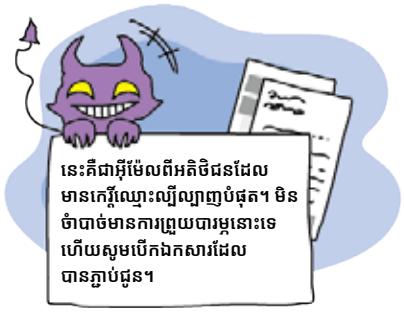
ស្វែងយល់បន្ថែមអំពីការគំរាមកំហែង និងវិធីសាស្ត្រវាយប្រហារ និងអនុវត្តជំហាននានាដើម្បីទប់ទល់នឹងបញ្ហានេះ។

មានការកើនឡើងនូវចំនួននៃការវាយប្រហារដោយការលួចបន្លំ (phishing attacks) ដើម្បីលួចយក ID និងលេខកូដសម្ងាត់តាមរយៈអ៊ីម៉ែលដែលមានមេរោគដោយធ្វើត្រាប់តាមដៃគូអាជីវកម្ម ឬភាគីពាក់ព័ន្ធដទៃផ្សេងទៀត ឬនាំឲ្យមនុស្សឲ្យចូលទៅកាន់វេបសាយក្លែងក្លាយ ដែលធ្វើត្រាប់តាមវេបសាយត្រឹមត្រូវស្របច្បាប់។ អនុវត្តជំហាននានាដើម្បីប្រយុទ្ធប្រឆាំងនឹងការគំរាមកំហែង និងវិធីសាស្ត្រវាយប្រហារដោយធ្វើការសិក្សាស្វែងយល់អំពីវា។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការត្រួតពិនិត្យវេបសាយ IPA និងចុះឈ្មោះក្នុង អ៊ីម៉ែល ដើម្បីសិក្សាស្វែងយល់អំពីការគំរាមកំហែង និងវិធីសាស្ត្រនៃការវាយប្រហារចុងក្រោយបំផុត និងការបញ្ជាក់អំពីការជូនដំណឹងដែលផ្តល់ជូនដោយសេវាធនាគារតាមអ៊ីនធឺណិត និងសេវាដទៃផ្សេងទៀតដែលកំពុងដាក់ឲ្យដំណើរការ។

ផ្នែកទី ២ វិធានការក្នុងនាមនិយោជិត

ចំណុចទី 6 ដល់ទី 18 គឺជាចំណុចដែលនិយោជិតគប្បីត្រូវដឹង។ កំហុសរបស់មនុស្សអាចកើតមានឡើងបានយ៉ាងងាយស្រួលដោយសារភាពស្រដៀងគ្នានៃការគ្រប់គ្រងព័ត៌មានសំខាន់ជារៀងរាល់ថ្ងៃ និងអាចបង្កឡើងដោយការមិនយកចិត្តទុកដាក់ចំពោះបញ្ហា។ បន្ថែមលើនេះ ដោយសារលក្ខណៈនៃការគំរាមកំហែងមានការប្រែប្រួលជារៀងរាល់ថ្ងៃ អ្នកត្រូវមានការប្រុងប្រយ័ត្ននៅគ្រប់ពេលទាំងអស់។



ចំណុចលេខ ៦ តារាងលេខ៦ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានអ៊ីម៉ែល

ត្រូវមានការសង្ស័យចំពោះអ៊ីម៉ែលដែលទទួលបានពីមនុស្សគ្រប់គ្នាដែលអ្នកមិនបានស្គាល់

នេះអាចនាំឲ្យមានការឆ្លងមេរោគដោយការបើកឯកសារភ្ជាប់ក្នុងអ៊ីម៉ែល ឬដោយធ្វើការចុចនៅលើតំណភ្ជាប់ URL នៅក្នុងអ៊ីម៉ែល។ ត្រូវមានការប្រុងប្រយ័ត្នចំពោះឯកសារភ្ជាប់ និងការចុចលើតំណភ្ជាប់ URL ពីអ្នកធ្វើដែលអ្នកពុំបានស្គាល់។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការមិនបើកឯកសារភ្ជាប់ ឬការមិនចុចលើតំណភ្ជាប់ URL នៅក្នុងអ៊ីម៉ែលដែលមានការសង្ស័យ និងធ្វើការរាយការណ៍អ៊ីម៉ែលដែលមានការសង្ស័យជូនដល់ផ្នែកសន្តិសុខ ដើម្បីធ្វើការចែករំលែកព័ត៌មានអំពីអ៊ីម៉ែលដែលមានការសង្ស័យនៅក្នុងក្រុមហ៊ុន។

ចំណុចលេខ ៧ តារាងលេខ៧ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានអ៊ីម៉ែល

ការបង្ការការធ្វើអ៊ីម៉ែលទៅខុសពីអ្នកទទួល

នឹងមានគ្រោះថ្នាក់នៃការលេចធ្លាយព័ត៌មានដល់មនុស្សចម្លែកដោយសារការធ្វើអ៊ីម៉ែលខុស ឬធ្វើទូរសារដល់មនុស្សខុស។ ត្រូវប្រាកដថាបានត្រួតពិនិត្យដោយប្រុងប្រយ័ត្នចំពោះអ្នកណាដែលត្រូវធ្វើអ៊ីម៉ែល និងធ្វើទូរសារទៅកាន់។ បន្ថែមលើនេះ ការលេចធ្លាយព័ត៌មានអាចកើតមានឡើងនៅពេលនៅពេលអ្នកធ្វើអ៊ីម៉ែលទៅអាសយដ្ឋានខុស។ នៅពេលធ្វើអ៊ីម៉ែលទៅមនុស្សច្រើននាក់ ត្រូវប្រាកដថាអាសយដ្ឋានអ្នកទទួលពិតជាត្រឹមត្រូវ។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការត្រួតពិនិត្យពីរដងលើអាសយដ្ឋាននៅមុនពេលធ្វើអ៊ីម៉ែល ឬធ្វើទូរសារ និងធ្វើការជ្រើសរើសអាសយដ្ឋានសម្រាប់ធ្វើ ចម្លងជូន (CC) និងធ្វើជូនដោយសម្ងាត់ (BCC) នៅក្នុងអ៊ីម៉ែល។

ចំណុចលេខ ៨ តារាងលេខ៨ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានអ៊ីម៉ែល

ការពារព័ត៌មានសំខាន់នៅពេលធ្វើអ៊ីម៉ែល

នៅពេលធ្វើព័ត៌មានសំខាន់តាមអ៊ីម៉ែល ហាមសរសេរវានៅក្នុងខ្លឹមសារអ៊ីម៉ែល។ ផ្ទុយទៅវិញ សរសេរវានៅក្នុងឯកសារ ការពារវាដោយលេខកូដសម្ងាត់ និងភ្ជាប់វាទៅក្នុងអ៊ីម៉ែល។ ជូនដំណឹងដល់អ្នកទទួលអ៊ីម៉ែលអំពីលេខកូដសម្ងាត់តាមការហៅទូរស័ព្ទ ឬតាមរយៈមធ្យោបាយផ្សេងទៀត ជាជាងការសរសេរវានៅក្នុងអ៊ីម៉ែល។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការសរសេរព័ត៌មានសំខាន់នៅក្នុងឯកសារ និងការពារវាដោយលេខកូដសម្ងាត់។ ជូនដំណឹងដល់អ្នកទទួលសារអំពីលេខកូដសម្ងាត់តាមទូរស័ព្ទ ឬតាមមធ្យោបាយផ្សេងទៀត។

ចំណុចលេខ ៩ តារាងលេខ៩ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានបណ្តាញឥតខ្សែ (Wireless LAN)

ការពារការលួចស្តាប់ និងការប្រើប្រាស់ដែលគ្មានការអនុញ្ញាតនៃបណ្តាញឥតខ្សែ (wireless LAN)

បណ្តាញឥតខ្សែ (Wireless LANs) ដែលពុំមានការការដំឡើងប្រព័ន្ធសន្តិសុខគ្រប់គ្រាន់អាចមានការលួចអានទិន្នន័យ ឬប្រើប្រាស់ពុំបានត្រឹមត្រូវសម្រាប់សកម្មភាពក្រិដ្ឋដោយការភ្ជាប់ដោយខុសច្បាប់ទៅកាន់បណ្តាញទាំងនោះ។ ត្រូវប្រាកដថាបានបានដំឡើងប្រព័ន្ធសន្តិសុខនៃបណ្តាញឥតខ្សែ (wireless LAN) ដើម្បីការពារការលួចស្តាប់ និងការប្រើប្រាស់ដែលគ្មានការអនុញ្ញាត។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាប្រើប្រាស់ការកំណត់បម្លែងកូដ (ឧ.ទា. WPA2-PSK) និងការប្រើប្រាស់លំដាប់ពាក្យសម្រាប់ចូលក្នុងប្រព័ន្ធ (pass phrase) ដែលមានលក្ខណៈវែង និងពិបាកក្នុងការទស្សទាយ។

ចំណុចលេខ ១០ តារាងលេខ១០ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានប្រើប្រាស់អ៊ីនធឺណិត

បង្ការបញ្ហានៅពេលប្រើប្រាស់អ៊ីនធឺណិត

ការចូលទៅមើលវេបសាយមានមេរោគ ឬវេបសាយដែលមានបញ្ហាសន្តិសុខអាចនាំឲ្យឧបករណ៍អេឡិចត្រូនិករបស់អ្នកឆ្លងមេរោគបាន។ បន្ថែមលើនេះ បណ្តាក្រុមហ៊ុននានាអាចទទួលរងគ្រោះថ្នាក់ដោយការបង្ហោះរឿងកំប្លែងនៅបណ្តាញព័ត៌មានសង្គម ឬផ្ទាំងផ្សព្វផ្សាយសារ ឬធ្វើការបង្ហោះព័ត៌មានសម្ងាត់ដោយចៃដន្យជាដើម។ វាជាការចាំបាច់ក្នុងការបង្ការគ្រោះថ្នាក់ដោយដាក់ឲ្យដំណើរការនូវប្រព័ន្ធមួយដែលរឹតបន្តឹងពីការប្រើប្រាស់អ៊ីនធឺណិតនៅកន្លែងការងារ។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការបង្កើតវិធានក្នុងការចូលទៅប្រើប្រាស់អ៊ីនធឺណិត និងបណ្តាញព័ត៌មានសង្គម និងប្រើប្រាស់កម្មវិធីរាំងខ្ទប់គេហទំព័រ (web filters) ដើម្បីធ្វើការរឹតបន្តឹងលើការប្រើប្រាស់អ៊ីនធឺណិតជាលក្ខណៈប្រព័ន្ធ។

ចំណុចលេខ ១១ តារាងលេខ១១ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានរក្សាទុកទិន្នន័យបម្រុង (Backup)

លើកទឹកចិត្តឲ្យមានការរក្សាទុកទិន្នន័យបម្រុង (backup) ជាប្រចាំ

ទិន្នន័យដែលបានរក្សាទុកនៅលើកុំព្យូទ័រ (PC) ឬម៉ាស៊ីនមេ (server) អាចបាត់បង់ដោយសារដំណើរការមិនប្រក្រតី ដំណើរការមានបញ្ហា ឬការឆ្លងមេរោគជាដើម។ ធ្វើការរក្សាទុកទិន្នន័យបម្រុង (backup) ដើម្បីត្រៀមសម្រាប់ស្ថានភាពដែលពុំបានព្រាងទុកមុន។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការអនុវត្តការរក្សាទុកទិន្នន័យបម្រុង (backup) នៃព័ត៌មានសំខាន់ៗជាប្រចាំថ្ងៃ និងការរក្សាទុកឯកសារទិន្នន័យបម្រុងនៅទីតាំងខុសៗគ្នា។

សេចក្តីពន្យល់

ចំណុចលេខ ១២ តារាងលេខ១២ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានរក្សាទុក

ព័ត៌មាន/ឯកសារសំខាន់ ត្រូវធ្វើការគ្រប់គ្រងឲ្យបានត្រឹមត្រូវ

វាមានគ្រោះថ្នាក់ណាស់ដែលទុកព័ត៌មាន/ឯកសារចោលដោយគ្មានអ្នកនៅមើលនៅលើតុ ដោយសារមនុស្សផ្សេងទៀតអាចយកវា ឬអានវាបាន។ ព័ត៌មាន/ឯកសារសំខាន់ ត្រូវធ្វើការគ្រប់គ្រងឲ្យបានត្រឹមត្រូវ ដើម្បីការពារកុំឲ្យអ្នកផ្សេងអាចមើលឃើញ ឬប៉ះកាន់វាបាន និងធានាថាព័ត៌មាននិងឯកសារទាំងនោះមិនត្រូវបានទុកចោលដោយគ្មានអ្នកមើលនោះទេ។ ត្រូវកំណត់ទីតាំងរក្សាទុកសម្រាប់ព័ត៌មាន/ឯកសារ យកវាចេញតែពេលណាចាំបាច់សម្រាប់ការងារតែប៉ុណ្ណោះ និងត្រូវធានាថាបានរក្សាទុកវានៅកន្លែងដើមវិញនៅពេលបញ្ចប់ការងាររួច។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការរៀបចំតុការងារឲ្យបានស្អាតនិងមានសណ្តាប់ធ្នាប់ និងការរក្សាទុកព័ត៌មាន/ឯកសារសំខាន់ៗនៅក្នុងទូរចាក់សោ។

ចំណុចលេខ ១៣ តារាងលេខ១៣ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានដឹកជញ្ជូន

ដឹកជញ្ជូនព័ត៌មានសំខាន់ក្នុងលក្ខណៈដែលមានសុវត្ថិភាព

នៅពេលយកព័ត៌មានសំខាន់ចេញក្រៅក្រុមហ៊ុន វាអាចត្រូវបានគេលួច ឬបាត់បង់ដោយប្រការណាមួយពុំបានដឹងមុន។ អនុវត្តជំហាននានាជាមុននៅពេលប្រើប្រាស់កុំព្យូទ័រយួរដៃ ឬទូរស័ព្ទស្មាតហ្វូន ដូចជាការកំណត់លេខកូដសម្ងាត់ ឬការកូដនីយកម្មឯកសារទិន្នន័យ ដើម្បីធានាថាព័ត៌មានពុំអាចពិនិត្យមើលបានដោយងាយស្រួលនៅក្នុងករណីត្រូវបានគេលួច ឬបាត់បង់។

វិធានការ៖ អនុវត្តវិធាននានា ដូចជាការកំណត់ជាចាំបាច់ក្នុងការទទួលបានការអនុញ្ញាតដើម្បីដឹកជញ្ជូនព័ត៌មានសំខាន់ ដោយរក្សាសន្តិសុខទិន្នន័យជាមួយលេខកូដសម្ងាត់នៅលើកុំព្យូទ័រយួរដៃ ទូរស័ព្ទស្មាតហ្វូន និង USB Drive និងមិនត្រូវទុកចោលអីវ៉ាន់ដោយគ្មានអ្នកនៅចាំមើលនោះទេ។

ចំណុចលេខ ១៤ តារាងលេខ១៤ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការគ្រប់គ្រងសុវត្ថិភាពការិយាល័យ

មិនត្រូវអនុញ្ញាតឲ្យអ្នកណាម្នាក់ប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកដោយគ្មានការអនុញ្ញាតនោះទេ

មិនត្រូវទុកកុំព្យូទ័រចោលដោយគ្មានអ្នកប្រើអំឡុងម៉ោងការងារនោះទេ។ កុំព្យូទ័រដែលគ្មានអ្នកប្រើអាចដំណើរការដោយអ្នកណាម្នាក់ ដូចជាអ្នកដែលអាចចូលទៅប្រើកុំព្យូទ័របានដោយគ្មានលេខកូដសម្ងាត់ជាដើម អាចប្រើកុំព្យូទ័រនេះពុំបានត្រឹមត្រូវ។ អនុវត្តជំហាននានាដើម្បីការពារកុំព្យូទ័រពីការប្រើប្រាស់ដែលគ្មានការអនុញ្ញាត។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការចាក់សោកុំព្យូទ័រនៅពេលអ្នកចាកចេញពីតុការងារ បិទកុំព្យូទ័រនៅពេលអ្នកចាកចេញពីកន្លែងការងារនៅពេលថ្ងៃ ការពារមនុស្សផ្សេងទៀតមិនឲ្យប្រើប្រាស់កុំព្យូទ័ររបស់អ្នក។

ចំណុចលេខ ១៥ តារាងលេខ១៥ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការគ្រប់គ្រងសុវត្ថិភាពការិយាល័យ

ចូលទៅជិតមនុស្សដែលអ្នកពុំធ្លាប់ស្គាល់

មានគ្រោះថ្នាក់នៃការលួចយកព័ត៌មាន ប្រសិនបើអ្នកមិនបានរឹតបណ្តឹងការចូលមកកាន់ការិយាល័យដោយមនុស្សដែលគ្មានការអនុញ្ញាត។ ត្រូវប្រាកដថាបុគ្គលដែលគ្មានការអនុញ្ញាតនោះ មិនត្រូវបានអនុញ្ញាតឲ្យចូលទៅកន្លែងរក្សាទុកព័ត៌មាន/ឯកសារសំខាន់ ជាពិសេសដូចជា ម៉ាស៊ីនមេ (servers) បណ្ណាសារ និងទូរដែកជាដើម។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការចូលទៅជិតអ្នកពុំធ្លាប់ស្គាល់ដែលចូលក្នុងការិយាល័យនៅកន្លែងតុទទួលភ្ញៀវ។

ចំណុចលេខ ១៦ តារាងលេខ១៦ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការគ្រប់គ្រងសុវត្ថិភាពការិយាល័យ

អនុវត្តជំហាននានាដើម្បីបង្ការការលួចសម្ភារៈនិងគ្រឿងបរិក្ខារផ្សេងៗ។

នៅពេលឧបករណ៍អេឡិចត្រូនិកដូចជាកុំព្យូទ័រយួរដៃ ថែបផ្លឺត និង USB Drive មានភាពងាយស្រួលនិងអាចចល័តបាន នោះក៏អាចធ្វើឲ្យវាប្រឈមនឹងគ្រោះថ្នាក់នៃការលួចយកផងដែរ។ នៅពេលឧបករណ៍ទាំងនេះមិនត្រូវបានប្រើប្រាស់ អនុវត្តជំហាននានាដើម្បីរក្សាទុកវានៅកន្លែងមានសុវត្ថិភាព ដូចជាក្នុងថតទូរចាក់សោជាដើម។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការចាក់សោកុំព្យូទ័រយួរដៃ ថែបផ្លឺត និងបរិក្ខារអេឡិត្រូនិកផ្សេងៗ (ស៊ីឌី USB Drive ហាដឌីសខាងក្រៅ (external hard drives) ។ល។) នៅក្នុងថតតុនៅពេលចាកចេញពីការិយាល័យនៅពេលថ្ងៃ។

ចំណុចលេខ ១៧ តារាងលេខ១៧ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការគ្រប់គ្រងសុវត្ថិភាពការិយាល័យ

ត្រូវមានការប្រុងប្រយ័ត្នក្នុងការចាក់សោការិយាល័យ

ការរក្សាទុកកំណត់ត្រាពេលវេលានៃបុគ្គលចុងក្រោយគេបំផុតដែលមានវត្តមាននៅការិយាល័យ ក៏អាចជួយលើកកម្ពស់ស្មារតីទំនួលខុសត្រូវឲ្យបុគ្គលដែលទៅក្រោយគេនោះចាក់សោទ្វារផងដែរ។ ព្យាយាមគ្រប់គ្រងកូនសោ និងកំណត់ត្រានានាឲ្យបានល្អ។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការគ្រប់គ្រងកូនសោនិងការរក្សាទុកកំណត់ត្រានៃបុគ្គលចុងក្រោយគេបំផុតដែលមានវត្តមាននៅក្នុងការិយាល័យដែលបានចាក់សោទ្វារ (កាលបរិច្ឆេទ ពេលវេលា និងឈ្មោះ)

ចំណុចលេខ ១៨ តារាងលេខ១៨ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការបោះចោលព័ត៌មានដោយសុវត្ថិភាព

លុបចោលព័ត៌មានសំខាន់ដើម្បីកុំឲ្យគេអាចស្តារវាមកវិញបាន

គ្រាន់តែការបោះចោលឯកសារដែលមានព័ត៌មានសំខាន់ចូលក្នុងធុងសំរាម ក៏អាចនាំឲ្យមានការលេចធ្លាយព័ត៌មានបានដែរ ដោយសារមនុស្សដទៃអាចអានឯកសារនោះបាន។ បន្ថែមលើនេះ ព័ត៌មានដែលបានរក្សាទុកនៅក្នុងឧបករណ៍អេឡិចត្រូនិក និងសារព័ត៌មានអេឡិចត្រូនិក អាចរក្សាទុកបាន បើទោះបីជាឯកសារទាំងនោះត្រូវបានលុបចោលក៏ដោយ។ នៅពេលបោះចោលព័ត៌មានសំខាន់ ត្រូវបោះវាចោលតាមវិធីណាមួយឲ្យបានត្រឹមត្រូវ ដូចជាការប្រើប្រាស់ម៉ាស៊ីនកាត់កម្ទេចក្រដាស ឬសូហ្វវែរលុបទិន្នន័យជាដើម។

វិធានការ៖ អនុវត្តជំហាននានាដើម្បីបោះចោលព័ត៌មាន ដូចជាការប្រើប្រាស់សូហ្វវែរលុបទិន្នន័យ ការបំផ្លាញរូបរាងសណ្ឋានរបស់វា ឬការស្នើសុំអ្នកជំនាញឲ្យធ្វើការលុបវាចោលជាដើម។

រក្សាទុកឯកសារដែលមានព័ត៌មានសំខាន់ៗនៅថតទូដែលមានចាក់សោ។

បង្ការការលួចឧបករណ៍អេឡិចត្រូនិក

ចាក់សោទ្វារការិយាល័យ

ផ្នែកទី ៣ វិធានការសម្រាប់ស្ថាប័ន

ចំណុច 19 ដល់ 25 គឺជាវិធានការនានាដែលត្រូវអនុវត្តបន្ទាប់ពីការបង្កើតគោលនយោបាយសម្រាប់ស្ថាប័នរួច។ លើកកម្ពស់ការយល់ដឹងរបស់និយោជិតដោយរៀបចំឯកសារវិធានសន្តិសុខព័ត៌មានឲ្យបានច្បាស់លាស់ និងចែករំលែកវិធាននោះនៅក្នុងការិយាល័យ។

ចំណុចលេខ ១៩ តារាងលេខ១៩ ស្វ័យវាយតម្លៃក្រុមហ៊ុនការជូនដំណឹងអំពីកាតព្វកិច្ចរបស់និយោជិតក្នុងការរក្សាព័ត៌មានសម្ងាត់

ឲ្យនិយោជិតយល់ដឹងពីកាតព្វកិច្ចរបស់ខ្លួនក្នុងការរក្សាព័ត៌មានសម្ងាត់

ទោះបីជាអ្នកខ្លះបានលើកឡើងថា វិធានក្រុមហ៊ុនបានតម្រូវឲ្យនិយោជិតរក្សាព័ត៌មានសម្ងាត់នៅក្នុងការងាររបស់ពួកគេរួចហើយក៏ពិតមែន ក៏ប៉ុន្តែវាជាការល្អក្នុងការជូនដំណឹងឲ្យបានច្បាស់អំពីវិធានរបស់ក្រុមហ៊ុនដើម្បីឲ្យពួកគេអនុវត្តតាម...

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការជូនដំណឹងដល់និយោជិតអំពីការរក្សាការសម្ងាត់នៅពេលពួកគេត្រូវបានជ្រើសរើសឲ្យបម្រើការងារ។

ចំណុចលេខ ២០ តារាងលេខ២០ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការបណ្តុះបណ្តាលនិយោជិត

រៀបចំការបណ្តុះបណ្តាលនិយោជិតជាប្រចាំ

និយោជិតអាចគ្រប់គ្រងព័ត៌មានជាប្រចាំថ្ងៃក្នុងពេលការងាររបស់ពួកគេ ហើយភាពស្រដៀងគ្នាមានន័យថា ពួកគេអាចមើលរំលងបញ្ហានេះ ហើយពួកគេអាចភ្លេចអំពីការគ្រប់គ្រងសន្តិសុខព័ត៌មានបាន។ ការបណ្តុះបណ្តាលនិយោជិតជាប្រចាំ គឺមានប្រសិទ្ធភាពក្នុងការបង្កើនការយល់ដឹងរបស់និយោជិត។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការពន្យល់ជាប្រចាំអំពីសារៈសំខាន់នៃការគ្រប់គ្រងព័ត៌មាន និងការបណ្តុះបណ្តាលបុគ្គលិកនៅក្នុងស្ថាប័ន។

ចំណុចលេខ ២១ តារាងលេខ២១ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកផ្ទាល់ខ្លួន

សម្រេចថាតើត្រូវអនុញ្ញាតឲ្យប្រើឧបករណ៍អេឡិចត្រូនិកផ្ទាល់ខ្លួនសម្រាប់បំពេញការងារដែរឬទេ

ត្រូវធានាថាសន្តិសុខមានភាពតឹងរឹង ប្រសិនបើមានការប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកផ្ទាល់ខ្លួន ដូចជា កុំព្យូទ័រ និងទូរស័ព្ទស្មាតហ្វូនសម្រាប់ធ្វើការងារ ដោយសារវាពិបាកក្នុងការគ្រប់គ្រងថាតើបុគ្គលិកប្រើប្រាស់ឧបករណ៍ទាំងនោះដោយរបៀបណា។ សម្រេចថាតើឧបករណ៍អេឡិចត្រូនិកផ្ទាល់ខ្លួនអាចប្រើប្រាស់សម្រាប់ធ្វើការងារបានដែរឬទេ និងត្រូវព្យាយាមកំណត់វិធានស្តីពីការប្រើប្រាស់ឧបករណ៍ទាំងនោះ។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការបង្កើតប្រព័ន្ធអនុញ្ញាតសម្រាប់ការប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកផ្ទាល់ខ្លួន ដូចជាកុំព្យូទ័រ និងទូរស័ព្ទស្មាតហ្វូនសម្រាប់ការងារ និងត្រូវកំណត់វិធាននានាសម្រាប់ការប្រើប្រាស់ឧបករណ៍ទាំងនោះ ប្រសិនបើអនុញ្ញាតឲ្យប្រើសម្រាប់បំពេញការងារ។

ចំណុចលេខ ២២ តារាងលេខ២២ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការគ្រប់គ្រងដៃគូអាជីវកម្ម

ស្នើសុំឲ្យដៃគូអាជីវកម្មឲ្យរក្សាការសម្ងាត់

ជៀសវាងការសន្មត់ថាដៃគូអាជីវកម្មនឹងរក្សាការសម្ងាត់ដោយឯកឯងផ្អែកលើលក្ខណៈនៃព័ត៌មាន។ នៅពេលផ្តល់ព័ត៌មានសម្ងាត់ដល់ដៃគូអាជីវកម្ម វាជាការចាំបាច់ក្នុងការបញ្ជាក់ឲ្យបានច្បាស់ថាព័ត៌មាននោះត្រូវរក្សាទុកជាការសម្ងាត់។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការធ្វើពង្រាងកិច្ចសន្យាដែលបញ្ជាក់ច្បាស់ពីការរក្សាទុកខ្លឹមសារជាការសម្ងាត់។

ចំណុចលេខ ២៣ តារាងលេខ២៣ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការប្រើប្រាស់សេវាពីខាងក្រៅ

ប្រើប្រាស់សេវាពីខាងក្រៅដែលអាចទុកចិត្តបាន

ប្រសិនបើអ្នកជ្រើសរើសសេវាពីខាងក្រៅ ដូចជាសេវាបច្ចេកវិទ្យាក្លាវដ៍ ដោយគិតគូរលើអាទិភាពនៃការចំណាយ អ្នកអាចកំណត់ឃើញថា សេវាទាំងនោះអាចមិនមានដោយសារមានកំហុសឬបញ្ហាណាមួយកើតឡើង។ ធ្វើការត្រួតពិនិត្យយ៉ាងហ្មត់ចត់ចំពោះការអនុវត្តការងារ ភាពអាចជឿទុកចិត្តបាន ព័ត៌មានលម្អិតអំពីសំណងការខូចខាត និងការពិចារណាផ្សេងទៀតនៅពេលប្រើប្រាស់សេវាពីខាងក្រៅសម្រាប់កម្មវិធីនានាដែលមានផលប៉ះពាល់យ៉ាងខ្លាំងដល់និរន្តរភាពអាជីវកម្ម។

វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការត្រួតពិនិត្យលក្ខខណ្ឌសេវាកម្ម ព័ត៌មានលម្អិតអំពីសំណងការខូចខាត វិធានការសន្តិសុខ និងអ្វីៗដែលពាក់ព័ន្ធផ្សេងទៀតនៅពេលជ្រើសរើសអាជីវករ។

សេចក្តីពន្យល់

ចំណុចលេខ ២៤	តារាងលេខ២៤ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើការត្រៀមសម្រាប់គ្រោះថ្នាក់ផ្នែកសន្តិសុខព័ត៌មាន

ត្រៀមរៀបចំជាមុនសម្រាប់គ្រោះថ្នាក់ផ្នែកសន្តិសុខព័ត៌មាន

នៅពេលមានគ្រោះថ្នាក់កើតមានឡើង ជាទូទៅពុំមានពេលសម្រាប់គិតឲ្យបានច្រើននោះទេ ហើយការពន្យារពេលក្នុងការឆ្លើយតបចំពោះគ្រោះថ្នាក់នេះ អាចបង្កើនផលប៉ះពាល់នៃគ្រោះថ្នាក់នោះ។ ប្រើប្រាស់គ្រោះថ្នាក់ដែលបានរាយការណ៍នៅក្នុងបណ្តាញព័ត៌មានជាសេចក្តីយោងដើម្បីគិតគូរថាតើអ្នកណានឹងត្រូវធ្វើអ្វី នៅពេលណា ដោយសន្មតថាមានរឿងដូចគ្នានេះបានកើតចំពោះក្រុមហ៊ុនរបស់អ្នក។

វិធានការ៖	វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការរៀបចំសៀវភៅណែនាំអំពីការឆ្លើយតបទៅនឹងការលេចធ្លាយ ការបាត់បង់ ឬការលួចព័ត៌មានសំខាន់ជាដើម។

ចំណុចលេខ ២៥	តារាងលេខ២៥ ស្វ័យវាយតម្លៃក្រុមហ៊ុនលើវិធានត្រៀមរៀបចំ

បង្កើតវិធាននានាសម្រាប់វិធានការសន្តិសុខព័ត៌មាន

បើទោះបីជានាយកប្រតិបត្តិបានដាក់ឲ្យដំណើរការគោលនយោបាយនានាសម្រាប់វិធានការសន្តិសុខព័ត៌មានក៏ពិតមែន (លើកលែងតែមានការរៀបចំឯកសារបានច្បាស់លាស់នៅក្នុងវិធានផ្ទៃក្នុង) ក៏និយោជិតត្រូវតែស្នើសុំការណែនាំពីអ្នកគ្រប់គ្រងរបស់ពួកគេនៅគ្រប់ពេលវេលាដែរ។ ដើម្បីអនុញ្ញាតឲ្យនិយោជិតអនុវត្តស្របទៅតាមវិធានស្តីពីការងាររបស់ពួកគេ វាចាំបាច់ក្នុងការរៀបចំឯកសារឲ្យបានច្បាស់លាស់ស្តីពី “វិធានក្រុមហ៊ុន” ដើម្បីឲ្យនិយោជិតអាចអានវាបាននៅគ្រប់ពេល។

វិធានការ៖	វិធានការ៖ អនុវត្តជំហាននានា ដូចជាការធ្វើឲ្យចំណុចពី ១-២៤ នៃតារាងវាយតម្លៃនេះក្លាយជាវិធានសម្រាប់វិធានការសន្តិសុខព័ត៌មាន និងចែករំលែកវានៅក្នុងក្រុមហ៊ុន និងធ្វើការត្រួតពិនិត្យឡើងវិញចំពោះវិធានទាំងនោះជាប្រចាំដើម្បីកែលម្អវានៅពេលរកឃើញថាមានការខ្វះចន្លោះនៅត្រង់ចំណុចណាមួយ។

NISC National center of Incident readiness and Strategy for Cybersecurity

IPA Information-technology Promotion Agency, Japan

2019.04