ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ
លេខ.០២២.......សហវ.ក.ប.ព

សេចក្តីណែនាំ
ស្តីពី
វិធានការទប់ស្កាត់ និង ឆ្លើយតបទៅនឹងការវាយប្រហារសាយប័រ លើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់អង្គភាពក្រោមឱវាទរដ្ឋមន្ត្រី និង ក្រោមអាណាព្យាបាល ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ

អង្គភាពក្រោមឱវាទរដ្ឋមន្ត្រី និង ក្រោមអាណាព្យាបាល ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ (ក.ស.ហ.វ.) បាន និង កំពុងប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានជាច្រើន សម្រាប់បម្រើដល់ការបំពេញការងារប្រចាំថ្ងៃ និង ការផ្តល់សេវាសាធារណៈ។ ក្នុងបរិការណ៍ដែលប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានបាន និង កំពុងដើរតួនាទីយ៉ាងសំខាន់ក្នុងការជំរុញប្រសិទ្ធភាពការងារ, ការគំរាមកំហែងពីការវាយប្រហារសាយប័របានក្លាយជាបញ្ហាប្រឈមដ៏ធំមួយដែលទាមទារការយកចិត្តទុកដាក់ខ្ពស់បំផុត។ ក្នុងស្មារតីបុរេសកម្ម, ក្រុមប្រឹក្សាបច្ចេកវិទ្យាព័ត៌មាន (ក.ប.ព.) នៃ ក.ស.ហ.វ. បានប្រមូលព័ត៌មានសំខាន់ៗ ពីប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់គ្រប់អង្គភាពទាំងអស់ ដើម្បីធ្វើការវាយតម្លៃសន្តិសុខឌីជីថលរបស់ប្រព័ន្ធនីមួយៗឡើងវិញ សំដៅដាក់ចេញនូវវិធានការទប់ស្កាត់ និង ឆ្លើយតបទៅនឹងការវាយប្រហារសាយប័រប្រកបដោយប្រសិទ្ធភាព និង ទាន់ពេលវេលា ជានាដល់ប្រក្រតីភាពនៃដំណើរការងារប្រចាំថ្ងៃរបស់ ក.ស.ហ.វ.។

ក. គោលបំណង

សេចក្តីណែនាំនេះ ត្រូវបានរៀបចំឡើងក្នុងគោលបំណងផ្តល់នូវវិធានការ និង នីតិវិធីប្រតិបត្តិជាស្តង់ដាច្បាស់លាស់ ដើម្បីការពារប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានពីការគំរាមកំហែងសាយប័រ។ សេចក្តីណែនាំនេះនឹងផ្តោតលើបញ្ហាចំពោះមុខដែលកំពុងជួបប្រទះ និង ចាំបាច់ត្រូវដោះស្រាយឱ្យខានតែបាន ព្រមទាំងផ្តោតលើការត្រៀមខ្លួន និង ប្រុងប្រយ័ត្នជាប្រចាំ ដើម្បីទប់ស្កាត់នឹងការប៉ុនប៉ងវាយប្រហារនៅថ្ងៃខាងមុខ។ ការអនុវត្តតាមសេចក្តីណែនាំនេះ នឹងមិនត្រឹមតែធានាបាននូវសុវត្ថិភាពទិន្នន័យ និង ហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាព័ត៌មានប៉ុណ្ណោះទេ ប៉ុន្តែថែមទាំងជួយរក្សាបាននូវស្ថិរភាពនៃដំណើរការការងារប្រចាំថ្ងៃ និង ចៀសវាងបាននូវផលវិបាក ដែលបណ្តាលមកពីការវាយប្រហារសាយប័រផងដែរ។ តាមរយៈការអនុវត្តរួមគ្នាប្រកបដោយការទទួលខុសត្រូវខ្ពស់, យើងនឹងអាចកសាងបាននូវប្រព័ន្ធការពារសាយប័ររឹងមាំមួយសម្រាប់ប្រព័ន្ធអេកូឡូស៊ីឌីជីថលរបស់ ក.ស.ហ.វ. ដែលអាចទប់ទល់នឹងបញ្ហាប្រឈមនានានៅក្នុងយុគសម័យឌីជីថលនេះ។ ដើម្បីសម្រេចបាននូវគោលបំណងនេះ, សេចក្តីណែនាំនេះដាក់ចេញនូវគោលដៅចំនួន ៤ រួមមាន៖

- កាត់បន្ថយភាពងាយរងគ្រោះធ្ងន់ធ្ងរ ដែលបានរកឃើញតាមរយៈការប្រមូលព័ត៌មានពីប្រព័ន្ធ និង ការរកឃើញហានិភ័យ តាមរយៈការវាយតម្លៃរបស់ក្រុមការងារបច្ចេកទេស,
- បង្កើតមូលដ្ឋានសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានសម្រាប់គ្រប់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានទាំងអស់ ដែលមានកំណត់ក្នុងវិសាលភាពនៃសេចក្តីណែនាំនេះ,

- ផ្តល់សេចក្តីណែនាំដល់ក្រុមការងារបច្ចេកទេស ក្នុងការធ្វើឱ្យប្រសើរឡើងនូវហេដ្ឋារចនាសម្ព័ន្ធ និង កម្មវិធីទៅកាន់កំណែថ្មី ដែលមានសុវត្ថិភាព, និង
- លើកកម្ពស់ការអនុវត្តសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានប្រកបដោយនិរន្តរភាពក្នុងចំណោមអ្នកគ្រប់គ្រងហេដ្ឋារចនាសម្ព័ន្ធ, អ្នកគ្រប់គ្រងប្រព័ន្ធ, អ្នកអភិវឌ្ឍកម្មវិធី និងអ្នកប្រើប្រាស់។

ខ. វិសាលភាព

សេចក្តីណែនាំនេះមានវិសាលភាពលើ៖

- គ្រប់បណ្តាអង្គភាព និង អគ្គនាយកដ្ឋានទាំងអស់ស្ថិតនៅក្រោមឱវាទរដ្ឋមន្ត្រី និង ក្រោមអាណាព្យាបាល ក.ស.ហ.វ.,
- គ្រប់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានទាំងអស់ រួមបញ្ចូលទាំងបណ្តាញតភ្ជាប់, វេបសាយ, ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ឬ ផតថលសម្រាប់បម្រើសេវាសាធារណៈ និង ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានសម្រាប់ធ្វើការផ្ទៃក្នុង, និង
- គ្រប់មន្ត្រី, មន្ត្រីកិច្ចសន្យា, មន្ត្រីលក្ខន្តិកៈ, បុគ្គលិកកិច្ចសន្យា ព្រមទាំងក្រុមហ៊ុនផ្តល់សេវាទាក់ទងនឹងការអភិវឌ្ឍ ឬ ថែទាំបណ្តាញតភ្ជាប់, វេបសាយ, ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ឬ ផតថលទាំងអស់។

គ. គោលការណ៍

សេចក្តីណែនាំនេះអនុវត្តដោយគោរពតាមគោលការណ៍៖

- ដោះស្រាយបញ្ហាប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានដែលកំពុងតែជួបបញ្ហា ឬ មានហានិភ័យខ្ពស់ប្រឈមនឹងការវាយប្រហារ,
- ត្រៀមខ្លួន និង បន្តពង្រឹងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ខ្លួនជាប្រចាំ ឱ្យបានរឹងមាំ និង មានសមត្ថភាពទប់ទល់នឹងការវាយប្រហារ, និង
- គោរពតាមវិធានការស្តង់ដាដែលបានដាក់ចេញឱ្យបានខ្ជាប់ខ្ជួន សំដៅកាត់បន្ថយនូវចន្លោះប្រហោងឱ្យបានជាអប្បបរមា។

ឃ. វិធានការដែលត្រូវអនុវត្ត

វិធានការដែលដាក់ចេញក្នុងសេចក្តីណែនាំនេះ បែងចែកក្រុមគោលដៅជា ៣ ក្រុម រួមមាន (១)-អ្នកគ្រប់គ្រងហេដ្ឋារចនាសម្ព័ន្ធ និង/ឬ មជ្ឈមណ្ឌលទិន្នន័យ, (២)-អ្នកគ្រប់គ្រង និង អ្នកអភិវឌ្ឍវេបសាយ, ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ឬ ផតថល និង (៣)-អ្នកប្រើប្រាស់ប្រព័ន្ធ។ ក្នុងនោះ វិធានការក៏ត្រូវបានកំណត់នូវអាទិភាព ដោយគិតពីស្ថានភាពដែលនាំឱ្យមានកម្រិតហានិភ័យខ្ពស់ និង ចាំបាច់ត្រូវដោះស្រាយឱ្យបានឆាប់រហ័ស រហូតដល់ស្ថានភាពដែលនាំឱ្យមានកម្រិតហានិភ័យទាប និង អាចបន្តដោះស្រាយជាអន្លើ។ វិធានការដែលត្រូវបានដាក់ចេញសម្រាប់ក្រុមគោលដៅទាំង ៣ ក្រុម រួមមានដូចខាងក្រោម៖

ក្រុមទី ១៖ អ្នកគ្រប់គ្រងហេដ្ឋារចនាសម្ព័ន្ធ និង/ឬ មជ្ឈមណ្ឌលទិន្នន័យ

សំដៅដល់ក្រុមមនុស្សដែលទទួលខុសត្រូវលើការត្រួតពិនិត្យ និង ថែទាំហេដ្ឋារចនាសម្ព័ន្ធដែលទ្រទ្រង់ដល់ដំណើរការប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរួមមាន គ្រប់គ្រងបណ្តាញតភ្ជាប់, មជ្ឈមណ្ឌលទិន្នន័យ, មជ្ឈមណ្ឌលសង្គ្រោះទិន្នន័យ និង ម៉ាស៊ីនមេ ជាដើម។ ក្នុងនោះ មជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន (Security Operation Center – SOC) ក៏រាប់បញ្ចូលនៅក្នុងក្រុមនេះដែរ។

ក្រុមនេះ ផ្តោតលើទិដ្ឋភាពការងារសំខាន់ៗ ដូចជា ការគ្រប់គ្រងបណ្តាញតភ្ជាប់, ការគ្រប់គ្រងមជ្ឈមណ្ឌលទិន្នន័យ, ការគ្រប់គ្រងម៉ាស៊ីនមេ និង ការគ្រប់គ្រងសមាសធាតុប្រព័ន្ធ ជាដើម។ វិធានការដែលបានដាក់ចេញសម្រាប់អ្នកគ្រប់គ្រងហេដ្ឋារចនាសម្ព័ន្ធ និង/ឬមជ្ឈមណ្ឌលទិន្នន័យ រួមមានដូចខាងក្រោម៖

១- កាត់បន្ថយផ្ទៃនៃការវាយប្រហារ (Attack Surface) ដោយកំណត់ឱ្យការចូលប្រើប្រាស់សេវាបានតែក្នុងចង្កោមអាសយដ្ឋានអាយភីរបស់ប្រទេសម្តុជា (IP Geo-Restriction) ប្រសិនបើមិនមានតម្រូវការចូលប្រើប្រាស់ជាសកលទេ,

២- បែងចែកបណ្តាញ (Network Segregation) ជាស្រទាប់ទៅតាមប្រភេទកម្មវិធី (Zone-based Architecture) រួមមានស្រទាប់សម្រាប់សេវា ឬ កម្មវិធីដែលត្រូវបើកឱ្យប្រើប្រាស់ជាសាធារណៈ (Public Zone (web/API)), ស្រទាប់សម្រាប់សេវាខាងក្នុង ឬ មុខងារស្នូលដែលមិនត្រូវបើកចេញខាងក្រៅ (Application/Business Logic Zone) និង ស្រទាប់ទុកទិន្នន័យ (Database Zone)។ ការបែងចែកនេះអាចរៀបចំជាទម្រង់បណ្តាញផ្ទៃក្នុងសិប្បនិម្មិត (VLAN) ដើម្បីបែងចែកស្រទាប់ទាំងនេះ ហើយការចូលប្រើប្រាស់ត្រូវឆ្លងកាត់ជញ្ជាំងការពារ (Firewall) ដែលកំណត់ការបើកឱ្យប្រើប្រាស់តែសេវាណាដែលចាំបាច់ត្រូវប្រើប្រាស់ (Service Whitelist),

៣- កំហិតការប្រើប្រាស់សេវាអ៊ីនធឺណិតចំពោះប្រព័ន្ធដែលផ្តល់សេវាផ្ទៃក្នុង លើកលែងតែសេវាមួយចំនួនដែលត្រូវការធ្វើបច្ចុប្បន្នកម្មជាមួយប្រព័ន្ធអ៊ីនធឺណិត ដូចជា សេវាធ្វើបច្ចុប្បន្នកម្មប្រព័ន្ធប្រតិបត្តិការ (Vendor Update Services) និង/ឬ សេវាដែលធ្វើសន្ធានកម្មជាមួយប្រព័ន្ធដទៃទៀតតាម អេភីអាយ (API),

៤- ទុកដាក់កូដកម្មវិធី និង ប្រព័ន្ធដំណើរការកម្មវិធីដែលបានតម្លើងរួច (Internal Software Repository and Image Registry) ឱ្យបានត្រឹមត្រូវក្នុងដែនបណ្តាញផ្ទៃក្នុង ចៀសវាងការទាញយកកូដ និង ប្រព័ន្ធដំណើរការកម្មវិធីទាំងនេះពីប្រព័ន្ធអ៊ីធឺណិតឱ្យបានជាអតិបរមា,

៥- បង្កើនភាពរឹងមាំលើម៉ាស៊ីនមេវេប (Web Server) ដោយបិទផ្ទាំងបង្ហាញកំណែរបស់កម្មវិធី (Banner Headers) លើម៉ាស៊ីនមេវេបដូចជា Apache, Nginx, SSH ជាដើម និង បិទមុខងារសម្រាប់បង្ហាញបញ្ជីផ្ទុកឯកសារ (Disable Directory Listing) ក៏ដូចជាបិទគេហទំព័រគំរូ (Default Pages) ដើម្បីកាត់បន្ថយការបង្ហាញព័ត៌មានមិនចាំបាច់ពីប្រព័ន្ធចេញទៅក្រៅ,

៦- បើកជញ្ជាំងការពារបន្ថែមទៀតកម្រិតប្រព័ន្ធប្រតិបត្តិការ (Host-Level Firewall) សម្រាប់ម៉ាស៊ីនមេទាំងអស់ ហើយកំណត់បទបញ្ជា (Rule) ចេញចូលប្រើប្រាស់សេវា ឱ្យបានច្បាស់លាស់,

៧- ដាក់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានសំខាន់ៗ មកមជ្ឈមណ្ឌលទិន្នន័យរួម ដោយមានក្រុមការងារ SOC នៅជួយគាំទ្រ,

៨- សហការជាមួយ ក.ប.ព. ដើម្បីដាក់កម្មវិធីសុវត្ថិភាព Endpoint Detection and Response (EDR) លើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានសំខាន់ៗ, និង

៩- ត្រូវកំណត់ជាកំហិតចំពោះការប្រើប្រាស់ពិធីសារសុវត្ថិភាពជំនាន់ចុងក្រោយ ដូចជា TLS 1.2/1.3 និង ត្រូវបញ្ឈប់ការប្រើប្រាស់កំណែជំនាន់ទាបជាងនេះ។

ក្រុមទី ២៖ អ្នកគ្រប់គ្រង និង អ្នកអភិវឌ្ឍ

សំដៅដល់ក្រុមមនុស្សដែលទទួលខុសត្រូវលើការរចនា, ការអភិវឌ្ឍ, ការដាក់ឲ្យដំណើរការ និង ការថែទាំរៀបសាយ, ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ឬ ផតថលនានា។ ក្នុងនោះ ក្រុមហ៊ុនផ្តល់សេវាពីខាងក្រៅ ដែលមានការទទួលខុសត្រូវដូចគ្នា ក៏រាប់បញ្ចូលនៅក្នុងក្រុមនេះដែរ។ ក្រុមនេះផ្តោតលើទិដ្ឋភាពការងារសំខាន់ៗ ដូចជា ការគ្រប់គ្រងសមាសធាតុអភិវឌ្ឍកម្មវិធី (Framework និង Library), ការពង្រឹងសុវត្ថិភាពប្រព័ន្ធ, ការកំណត់សុវត្ថិភាព(Configuration Security) ព្រមទាំងការថតចំលងប្រព័ន្ធទុក (Backup) និង ការស្តារប្រព័ន្ធឡើងវិញ (Restore)។ វិធានការដែលបានដាក់ចេញសម្រាប់អ្នកគ្រប់គ្រង និង អ្នកអភិវឌ្ឍប្រព័ន្ធ រួមមានដូចខាងក្រោម៖

១- ធ្វើបច្ចុប្បន្នកម្មសមាសធាតុសុសវែរជំនាន់ចាស់ៗ ដែលងាយរងគ្រោះ មកកំណែជំនាន់ថ្មីដែលមានសុវត្ថិភាពខ្ពស់។ **សូមទាក់ទង ក.ប.ព. ដើម្បីបានបញ្ជីនៃប្រព័ន្ធដែលត្រូវធ្វើបច្ចុប្បន្នកម្មសុសវែរមកជំនាន់ដែលមានសុវត្ថិភាព,**

២- គ្រប់គ្រងការធ្វើបច្ចុប្បន្នកម្មនៃការបិទចន្លោះប្រហោង (Patch Management) ដែលបានរកឃើញក្នុងប្រព័ន្ធ ដោយរក្សាកំណត់ហេតុនៃការធ្វើបច្ចុប្បន្នកម្ម (System Update/ Software Patch Log) នៅកន្លែងរួមណាមួយដែលផ្តល់ភាពងាយស្រួលសម្រាប់ការតាមដាន និង ត្រូវធ្វើស្វ័យប្រវត្តិកម្មជាមួយការធ្វើបច្ចុប្បន្នកម្មប្រព័ន្ធប្រតិបត្តិការ និងសមាសភាពសុសវែរផ្សេងៗ (OS and Software Component Patching),

៣- វាយតម្លៃភាពងាយរងគ្រោះជាប្រចាំ (Vulnerability Assessment) ដោយអនុវត្តការស្កែនប្រចាំត្រីមាសដោយប្រើឧបករណ៍វាយតម្លៃភាពងាយរងគ្រោះបើកចំហរ (ឧ. OpenVAS) ឬទាក់ទង ក.ប.ព. ដើម្បីពិនិត្យលទ្ធភាពដាក់បញ្ចូលប្រព័ន្ធចូលក្នុងប្រព័ន្ធកណ្តាលសម្រាប់វាយតម្លៃភាពងាយរងគ្រោះ។ ក្នុងនោះសូមពិនិត្យ និង ផ្តល់អាទិភាពដល់ភាពងាយរងខ្ពស់ (High Risk) សម្រាប់ការកែតម្រូវក្នុងរយៈពេលដែលបានកំណត់ណាមួយ បន្ទាប់ពីទទួលបានការវាយតម្លៃភាពងាយរងគ្រោះរួចហើយ និង ត្រូវធ្វើការវាយតម្លៃឡើងវិញបន្ទាប់ពីធ្វើការកែតម្រូវរួចរាល់ (Re-scan for Vulnerabilities),

៤- រៀបចំផែនការសម្រាប់ធានាដល់ប្រក្រតីភាពនៃដំណើរការប្រព័ន្ធ (Business Continuity Plan) តាមរយៈការចម្លងទុក (Backup) ប្រព័ន្ធ និង ទិន្នន័យជាប្រចាំ, ការរៀបចំផែនការស្តារប្រព័ន្ធឡើងវិញ (Disaster Recovery Planning) និងការសាកល្បងស្តារប្រព័ន្ធ និងទិន្នន័យឡើងវិញ ដើម្បីធានាពីភាពប្រក្រតីនៃប្រព័ន្ធ និង ទិន្នន័យដែលបានចម្លង,

៥- រៀបចំឯកសារស្តារប្រព័ន្ធឡើងវិញ និង ធ្វើបច្ចុប្បន្នភាពជាប្រចាំនូវឯកសារនេះ (Disaster Recovery Plan Document) ដែលរួមមាន ព័ត៌មាន និង ទំនាក់ទំនងម្ចាស់ប្រព័ន្ធ (System Owners) ដើម្បីអាចទាក់ទងបានពេលមានបញ្ហាប្រព័ន្ធ, ជំហាននៃការស្តារប្រព័ន្ធឡើងវិញ (Recovery Steps) និង រៀបចំព័ត៌មានទំនាក់ទំនងថ្នាក់ដឹកនាំទទួលបន្ទុកក្នុងករណីមានបញ្ហាដែលត្រូវការការសម្រេចចិត្តភ្លាមៗ,

៦- ត្រួតពិនិត្យ និង ថែទាំប្រព័ន្ធជាប្រចាំដោយចាត់តាំងក្រុមការងារទទួលបន្ទុកតាមដាន និង ត្រួតពិនិត្យប្រព័ន្ធ ហើយរៀបចំឱ្យមានការតាមដានមើលដំណើរការនៃប្រព័ន្ធ (Availability Monitoring) និង ភាពមិនប្រក្រតីនៃប្រព័ន្ធ (Anomaly Detection)។ ទិន្នន័យប្រវត្តិព្រឹត្តិការណ៍ទាំងនេះគួរតែរក្សាទុកនៅកន្លែងរួមតែមួយផ្ទាល់ខ្លួន ដើម្បីមានលទ្ធភាពក្នុងការស្រាវជ្រាវពេលមានភាពមិនប្រក្រតីកើតឡើង ឬ កំណត់ដាក់ប្រព័ន្ធរបស់ខ្លួនដើម្បីបញ្ជូនព័ត៌មានទាំងនេះទៅកាន់ SOC ដើម្បីត្រួតពិនិត្យ និង តាមដានដោយក្រុមការងារជំនាញ,

៧- កំហិតការប្រើប្រាស់គណនីដែលមានសិទ្ធជាអ្នកគ្រប់គ្រងប្រព័ន្ធ ចូលប្រើប្រាស់ប្រព័ន្ធតាមអ៊ីនធឺណិត និង លើកទឹកចិត្តឲ្យប្រើប្រាស់សម្រាប់តែក្នុងបណ្តាញខាងក្នុង។ ក្នុងករណី មានតម្រូវការចាំបាច់ត្រូវបើកការចូលប្រើប្រាស់ពីខាងក្រៅបណ្តាញ ត្រូវគិតគូរប្រើប្រាស់លេខសំងាត់ដែលរឹងមាំ ជាមួយការផ្ទៀងផ្ទាត់ពហុកត្តា (Multi-Factor Authentication) ឬប្រើប្រាស់ថ្នាល CamDigiKey,

៨- ប្រើប្រាស់ការផ្ទៀងផ្ទាត់ពហុកត្តា (Multi-Factor Authentication) និង ខេបចា (CAPTCHA) សម្រាប់គ្រប់ប្រព័ន្ធដែលប្រើប្រាស់គណនីទម្រង់ឈ្មោះ និង លេខសំងាត់ សម្រាប់ចូលប្រើប្រាស់ជាសាធារណៈ ឬត្រូវធ្វើសន្ធានកម្មជាមួយកម្មវិធី CamDigiKey,

៩- កំណត់លេខសំងាត់ដែលរឹងមាំសម្រាប់គណនីអ្នកប្រើប្រាស់ ដែលយ៉ាងហោចណាស់ត្រូវមាន ៨ អក្សរ/លេខ/អក្សរពិសេស សម្រាប់លេខសំងាត់ ហើយគួរមានថ្ងៃផុតកំណត់រាល់ ៦០ ទៅ ៩០ ថ្ងៃម្តងដើម្បីផ្លាស់ប្តូរ និង ត្រូវមានលទ្ធភាពក្នុងការបិទការចូលប្រើប្រាស់ប្រព័ន្ធពេលមានការវាយលេខសំងាត់ខុសច្រើនដង,

១០- មិនគួរមានគណនីរួមសម្រាប់អ្នកគ្រប់គ្រងប្រព័ន្ធឡើយ; ត្រូវមានគណនីដាច់ដោយឡែកដែលអាចកំណត់សិទ្ធិប្រើប្រាស់ និង មានលទ្ធភាពក្នុងការតាមដានការប្រើប្រាស់គណនីរបស់អ្នកគ្រប់គ្រងម្នាក់ៗ។ ការកំណត់តួនាទី និង សិទ្ធអ្នកប្រើប្រាស់ត្រូវគិតគូរឱ្យបានច្បាស់លាស់ ដោយឈរលើគោលការណ៍អនុញ្ញាតតែសិទ្ធិដែលត្រូវការចាំបាច់ (Least Privilege Principle),

១១- បិទការចូលប្រើប្រាស់ពីសាធារណៈនូវច្រកប្រើប្រាស់សេវាដែលមានហានិភ័យខ្ពស់ (Block High-risk Ports) ដើម្បីបង្រួមផ្ទៃនៃការវាយប្រហារ (Reduce Attack Surface) ឲ្យនៅកម្រិតអប្បបរមា ដែលមានដូចជា TCP 22, 3389, 3306, 1433, 5432, 1521 ជាដើម។

ក្រុមទី ៣៖ អ្នកប្រើប្រាស់ប្រព័ន្ធ

សំដៅដល់គ្រប់មន្ត្រី, មន្ត្រីកិច្ចសន្យា, មន្ត្រីលក្ខន្តិក: និង បុគ្គលិកកិច្ចសន្យា ដែលជាអ្នកប្រើប្រាស់ប្រព័ន្ធ ដើម្បីផ្តល់សេវា ឬបំពេញកិច្ចការប្រចាំថ្ងៃរបស់ខ្លួនដោយផ្ទាល់ក្តី ឬជាអ្នកប្រើប្រាស់ដោយប្រយោលក្តី។ ក្រុមនេះ ផ្តោតលើទិដ្ឋភាពសំខាន់ៗ ដូចជា ការផ្ទៀងផ្ទាត់អត្តសញ្ញាណចូលប្រើប្រាស់ប្រព័ន្ធដែលមានសុវត្ថិភាព, ការយល់ដឹងអំពីការប្រើប្រាស់ប្រព័ន្ធ និងការរាយការណ៍អំពីឧប្បត្តិហេតុដែលកើតឡើងភ្លាមៗ ជាដើម។ វិធានការដែលបានដាក់ចេញសម្រាប់អ្នកប្រើប្រាស់ រួមមានដូចខាងក្រោម៖

១- អ្នកប្រើប្រាស់ប្រព័ន្ធត្រូវប្រើប្រាស់ឧបករណ៍របស់ស្ថាប័ន ដោយមានស្មារតីទទួលខុសត្រូវខ្ពស់ និង ត្រូវសិក្សាស្វែងយល់បន្ថែមអំពីការប្រើប្រាស់ប្រព័ន្ធដោយសុវត្ថិភាពដូចជា៖ (ក)-ការវាយប្រហារលើអ្នកប្រើប្រាស់ដូចជាការវាយប្រហារបន្លំ (Phishing), (ខ)-ការការពារឧបករណ៍ខ្លួនពីការឆ្លងមេរោគ, (គ)-ចៀសវាងដំឡើងនូវកម្មវិធីដែលមិនមានប្រភពច្បាស់លាស់ ឬមិនមានអាជ្ញាបណ្ណត្រឹមត្រូវ, (ឃ)-ការធ្វើបច្ចុប្បន្នភាពកម្មវិធី និង ប្រព័ន្ធប្រតិបត្តិការឱ្យបានទៀងទាត់, (ង)-ការចៀសវាងការប្រើប្រាស់ USB ឬឧបករណ៍ផ្ទុកទិន្នន័យដែលមិនស្គាល់ប្រភព, (ច)-ការចៀសវាងចូលប្រើប្រាស់គេហទំព័រដែលគួរឱ្យសង្ស័យ, និង (ឆ)-ការចៀសវាងប្រើប្រាស់ឧបករណ៍របស់ស្ថាប័ន ភ្ជាប់ជាមួយវាយហ្វាយសាធារណៈ (Public Wifi) ដើម្បីវាយលេខកូដសំងាត់ចូលប្រើប្រាស់ប្រព័ន្ធ ឬបញ្ចូលព័ត៌មានសំងាត់ផ្សេងៗ, និង

២- អ្នកប្រើប្រាស់ប្រព័ន្ធត្រូវរាយការណ៍ទៅកាន់មន្ត្រីបច្ចេកទេស ឬក្រុមការងារសន្តិសុខបច្ចេកវិទ្យាពីសកម្មភាពគួរឱ្យសង្ស័យ ឬការវាយប្រហារដែលកើតមាន។ ភាពមិនប្រក្រតីមួយចំនួនរួមមាន៖ (ក)-គេហទំព័រស្ថាប័នត្រូវបានផ្លាស់ប្តូររូបភាពទាំងស្រុង ដែលមិនឆ្លុះបញ្ចាំងការងារបច្ចុប្បន្ន, (ខ)-គេហទំព័រចូលប្រើប្រាស់ប្រព័ន្ធត្រូវបានកំណត់ថាមិនមានសុវត្ថិភាពដោយកម្មវិធីបើកគេហទំព័រ (Browser), (ឃ)-ទទួលបានសារបន្លំ (Phishing) និង (ង)-សំគាល់ឃើញភាពដំណើរការយឺតខ្លាំងនៃប្រព័ន្ធ។

៦. យន្តការអនុវត្ត និង គាំទ្រ

គ្រប់អង្គភាព និង អគ្គនាយកដ្ឋានត្រូវរៀបចំក្រុមការងារបច្ចេកទេស ដើម្បីដោះស្រាយបញ្ហា, រៀបចំផែនការ និង គាំទ្រដល់ការអនុវត្តតាមសេចក្តីណែនាំនេះ ឱ្យបានហ៊ាស និង ហ្មត់ចត់បំផុត។ កិច្ចការអាទិភាពដែលបានកំណត់នៅក្នុងសេចក្តីណែនាំនេះ ត្រូវធ្វើឱ្យបានយ៉ាងយូរត្រឹមរយៈពេល ១ ខែ ដោយគិតចាប់ពីថ្ងៃដែលដាក់ចេញសេចក្តីណែនាំនេះ។ កិច្ចការមួយចំនួនទៀតនៅក្នុងសេចក្តីណែនាំនេះ ត្រូវយកចិត្តទុកដាក់ធ្វើជាប្រចាំ និង ត្រូវរៀបចំផែនការឱ្យបានច្បាស់លាស់ ដើម្បីការអនុវត្តប្រកបដោយប្រសិទ្ធភាព។ ក.ប.ព. ដែលមានក្រុមការងារនាយកដ្ឋានបច្ចេកវិទ្យាព័ត៌មាននៃអគ្គលេខាធិការដ្ឋានជាសេនាធិការ មានតួនាទីដឹកនាំ, សម្របសម្រួល និង គាំទ្រ។

ទទួលបានសេចក្តីណែនាំនេះ, គ្រប់អង្គភាព និង អគ្គនាយកដ្ឋានពាក់ព័ន្ធទាំងអស់ ត្រូវទទួលបន្ទុកអនុវត្តឱ្យមានប្រសិទ្ធភាព និង ស្មារតីទទួលខុសត្រូវខ្ពស់។

ថ្ងៃចន្ទ ១១រោច ខែអាសាឍ ឆ្នាំ ម្សាញ់ សប្តស័ក ព.ស. ២៥៦៩
រាជធានីភ្នំពេញ ថ្ងៃទី ១៤ ខែកក្កដា ឆ្នាំ ២០២៥