សុវត្ថិភាពទិន្នន័យ

សុវត្ថិភាពទិន្នន័យគឺជាដំណើរការនៃការការពារព័ត៌មានឌីជីថលពីការលួច ឬការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត។ សុវត្ថិភាពទិន្នន័យគ្របដណ្តប់លើ Hardware, Software, ឧបករណ៍ផ្ទុក និងឧបករណ៍អ្នកប្រើប្រាស់, ការចូលប្រើប្រាស់និងការគ្រប់គ្រងរដ្ឋបាល, ប្រតិបត្តិការហិរញ្ញវត្ថុ, គោលនយោបាយ និងនីតិវិធីរបស់ស្ថាប័នជាដើម។ ស្របពេលនឹងការវិវត្តយ៉ាងឆាប់រហ័សនៃបច្ចេកវិទ្យា សុវត្ថិភាពទិន្នន័យបានក្លាយជាមូលដ្ឋានគ្រឹះនៃបច្ចេកវិទ្យាព័ត៌មាន ដែលបានដើរតួនាទីយ៉ាងសំខាន់ក្នុងការការពារព័ត៌មានរសើបពីការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត ការប្រើប្រាស់មិនត្រឹមត្រូវ ឬការលួចព័ត៌មានជាដើម។ អាស្រ័យហេតុនេះ ទើបម្ចាស់អាជីវកម្ម រដ្ឋាភិបាល និងបុគ្គលបានពឹងផ្អែកយ៉ាងខ្លាំងលើថ្នាលឌីជីថលដើម្បីរក្សាទុក និងផ្លាស់ប្តូរទិន្នន័យ ដើម្បីការការពារទិន្នន័យនោះពីការគំរាមកំហែងនានាតាមប្រព័ន្ធអ៊ីនធឺណិត។ សុវត្ថិភាពទិន្នន័យរួមបញ្ចូលនូវការអនុវត្តបច្ចេកវិទ្យា និងគោលនយោបាយជាច្រើនដែលត្រូវបានរចនាឡើង ដើម្បីធានាឱ្យបាននូវភាពសម្ងាត់ (Confidentiality), សុចរិតភាព (Integrity) និងលទ្ធភាពដែលអាចប្រើប្រាស់បាន (Availability)។ ចំពោះ Confidentially ឬការសម្ងាត់សំដៅលើការរឹតបន្តឹងការចូលប្រើទិន្នន័យសម្រាប់តែបុគ្គល ឬប្រព័ន្ធដែលមានការអនុញ្ញាតប៉ុណ្ណោះ។ Integrity ធានាថាទិន្នន័យនៅតែមានភាពត្រឹមត្រូវ និងមិនមានការផ្លាស់ប្តូរអំឡុងពេលផ្ទុក ឬបញ្ជូន ខណៈពេលដែលលទ្ធភាពដែលប្រើប្រាស់បានធានាថាអ្នកប្រើប្រាស់ដែលមានការអនុញ្ញាតអាចចូលប្រើទិន្នន័យបានគ្រប់ពេលវេលា។ តម្រូវការសម្រាប់សុវត្ថិភាពទិន្នន័យត្រូវបានពង្រីកដោយកំណើនអិចស្ប៉ូណង់ស្យែលនៃព័ត៌មានឌីជីថល និងការកើនឡើងនៃភាពស្មុគស្មាញនៃការគំរាមកំហែងតាមអ៊ីនធឺណិត។ ការវាយប្រហារតាមអ៊ីនធឺណិត ដូចជា ការបន្លំ, Virus, Ransomware និងការវាយប្រហារ DDoS បានក្លាយជាកត្តាមួយដែលស្ថាប័នទាំងអស់មិនថាតូច ឬធំត្រូវតែយកចិត្តទុកដាក់។ ជាក់ស្តែង ការរំលោភលើទិន្នន័យដែលមានទម្រង់ធំ ដែលធ្លាប់កើតមានឡើង ដោយ Equifax, Yahoo, និង Marriott International បានលាតត្រដាងព័ត៌មានផ្ទាល់ខ្លួនរបស់បុគ្គលរាប់លាននាក់ ដែលបណ្តាលឱ្យខូចខាតផ្នែកហិរញ្ញវត្ថុ និងកេរ្តិ៍ឈ្មោះដល់អង្គភាពដែលរងផលប៉ះពាល់ និងជាពិសេសប៉ះពាល់ទៅលើអតិថិជនផងដែរ។ បន្ថែមពីនេះ បច្ចុប្បន្ន មនុស្សជាច្រើនបានធ្វើការផ្លាស់ប្តូរទៅប្រើប្រាស់បច្ចេកវិទ្យាក្លោដសម្រាប់ការផ្ទុកទិន្នន័យផ្សេងៗ និងការធ្វើការងារពីចម្ងាយ ដែលបានធ្វើឱ្យមានភាពស្មុគស្មាញបន្ថែមទៀតដល់ទិដ្ឋភាពនៃសុវត្ថិភាពទិន្នន័យ។ ខណៈពេលដែលបច្ចេកវិទ្យាក្លោដត្រូវបានប្រើប្រាស់ជាសកល បច្ចេកវិទ្យានេះបានក្លាយជាកន្លែងប្រមូលផ្តុំទិន្នន័យរសើបមួយចំនួនធំផងដែរ ដែលធ្វើឱ្យពួកគេក្លាយជាគោលដៅចម្បងសម្រាប់អ្នកវាយប្រហារ។ ដើម្បីទប់ទល់នឹង

ហានិភ័យទាំងនេះ ស្ថាប័នទាំងអស់បានអនុវត្តវិធានការសុវត្ថិភាពផ្សេងៗ រួមទាំង Encryption, Firewalls, ប្រព័ន្ធស្វែងរកការវាយប្រហារ និង Multi-factor Authentication ជាដើម។ បន្ថែមពីនេះ គោលការណ៍សុវត្ថិភាពទិន្នន័យ ដូចជា ការធ្វើបច្ចុប្បន្នភាពកម្មវិធីទៀងទាត់ ការបណ្តុះបណ្តាលបុគ្គលិក និងការគ្រប់គ្រងការចូលប្រើប្រាស់ទិន្នន័យ គឺជាកត្តាចាំបាច់ដើម្បីកាត់បន្ថយភាពងាយរងគ្រោះ។ ក្រុមហ៊ុនផ្តល់សេវា ក្លោដ និងក្រុមហ៊ុនបច្ចេកវិទ្យាក៏បាននិងកំពុងវិនិយោគយ៉ាងច្រើននៅក្នុងឧបករណ៍កម្រិតខ្ពស់ ដូចជា បញ្ញាសិប្បនិម្មិត និងម៉ាស៊ីនសិក្សា ដើម្បីស្វែងរក និងឆ្លើយតបទៅនឹងការគំរាមកំហែងក្នុងពេលជាក់ស្តែងផងដែរ។

I. ទំនាក់ទំនងរវាងសុវត្ថិភាពទិន្នន័យ, ឯកជនភាពទិន្នន័យ និងសុវត្ថិភាពអ៊ីនធឺណិត

នៅក្នុងយុគសម័យឌីជីថល មនុស្សពឹងផ្អែកយ៉ាងខ្លាំងលើការប្រើប្រាស់ថ្នាលឌីជីថលសម្រាប់ការ ទំនាក់ទំនង ផ្ទុកទិន្នន័យ និងធ្វើប្រតិបត្តិការនានានៅលើអ៊ីនធឺណិត ដែលជាហេតុធ្វើឱ្យការធានាការពារទិន្នន័យមានសារៈសំខាន់នាពេលបច្ចុប្បន្ននេះ។ ការធានានូវសុវត្ថិភាព និងការទទួលខុសត្រូវចំពោះការគ្រប់គ្រងព័ត៌មាននៅក្នុងទិដ្ឋភាពឌីជីថល បានធ្វើឱ្យលេចចេញនូវទំនាក់ទំនងរវាងសុវត្ថិភាពទិន្នន័យ, ឯកជនភាពទិន្នន័យ និងសុវត្ថិភាពអ៊ីនធឺណិត ដែលសមាសធាតុទាំងបីនេះបង្កើតបានជាការការពារដ៏មានប្រសិទ្ធភាពមួយប្រឆាំងនឹងហានិភ័យដែលកំពុងវិវត្តន៍នៅក្នុងទិដ្ឋភាពឌីជីថលដោយធានាបាននូវភាពត្រឹមត្រូវ ការសម្ងាត់ និងឯកជនភាពនៃទិន្នន័យនៅទូទាំងប្រព័ន្ធអនឡាញ។ សុវត្ថិភាពទិន្នន័យផ្តោតលើការការពារទិន្នន័យពីការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត និងការរំលោភបំពាននានា តាមរយៈវិធីសាស្ត្រ ដូចជា ការធ្វើ Encryption, ការគ្រប់គ្រងការចូលប្រើប្រាស់ និងប្រព័ន្ធបម្រុងទុក (Backup System)។ ចំណែកឯ ឯកជនភាពទិន្នន័យ សង្កត់ធ្ងន់ទៅលើក្រមសីលធម៌ និងច្បាប់នៃការគ្រប់គ្រងទិន្នន័យផ្ទាល់ខ្លួន ដោយធានាថាបុគ្គលម្នាក់ៗមានការគ្រប់គ្រងលើរបៀបដែលព័ត៌មានរបស់ពួកគេត្រូវបានប្រមូល ប្រើប្រាស់ និងចែករំលែក។ ចំពោះសុវត្ថិភាពអ៊ីនធឺណិត ផ្តោតសំខាន់លើការការពារទាំងសុវត្ថិភាពទិន្នន័យ និងឯកជនភាព ដោយការពារប្រព័ន្ធ, បណ្តាញ និងទិន្នន័យពីការគំរាមកំហែងតាមអ៊ីនធឺណិត ជាពិសេសនៅពេលដែលទិន្នន័យត្រូវបានបញ្ជូននៅលើអ៊ីនធឺណិត។ សមាសធាតុទាំងបីនេះមានទំនាក់ទំនងប្រទាក់ក្រឡាជាមួយគ្នា ហើយការភ្ជាប់ទំនាក់ទំនងគ្នារវាងសុវត្ថិភាពទិន្នន័យ ឯកជនភាពទិន្នន័យ និងសុវត្ថិភាពអ៊ីនធឺណិតនឹងត្រូវបានបង្ហាញនៅខាងក្រោមនេះ៖

◉ ការគាំទ្រពីសុវត្ថិភាពទិន្នន័យចំពោះឯកជនភាពទិន្នន័យ

ឯកជនភាពទិន្នន័យមិនអាចកើតឡើងបានឡើយ ប្រសិនបើគ្មានការគាំទ្រពីសុវត្ថិភាពទិន្នន័យ ដោយហេតុថាសុវត្ថិភាពទិន្នន័យគឺជាមូលដ្ឋានគ្រឹះដ៏សំខាន់ ដើម្បីការពារព័ត៌មានផ្ទាល់ខ្លួនពីការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត ឬការរំលោភបំពានទិន្នន័យ។ អ្នកប្រើប្រាស់ទូទៅ ឬស្ថាប័ននានាគួរតែអនុវត្តវិធីសាស្ត្ររួមដែលរួមបញ្ចូលគ្នានូវការអនុវត្តឯកជនភាពទិន្នន័យ ដូចជា Consent

Management និង Data Subject Rights ជាដើម ជាមួយនឹងវិធានការសុវត្ថិភាពទិន្នន័យខ្លាំង ដូចជា Encryption, ការគ្រប់គ្រងការចូលប្រើប្រាស់ និងការកំណត់ការគំរាមកំហែងជាដើម ដើម្បីធានាថាទិន្នន័យផ្ទាល់ខ្លួនមិនត្រឹមតែត្រូវបានគ្រប់គ្រងដោយគោរពតាមគោលការណ៍ឯកជនភាពប៉ុណ្ណោះទេ ប៉ុន្តែថែមទាំងត្រូវបានការពារពីការគំរាមកំហែងដែលអាចកើតមានផងដែរ។

● សុវត្ថិភាពទិន្នន័យពឹងផ្អែកលើសុវត្ថិភាពអ៊ីនធឺណិត

នាពេលបច្ចុប្បន្ន ជាញឹកញាប់ទិន្នន័យត្រូវបានបញ្ជូនតាមរយៈអ៊ីនធឺណិត ហើយប្រសិនបើគ្មានវិធានការសុវត្ថិភាពអ៊ីនធឺណិតត្រឹមត្រូវ ទិន្នន័យគឺងាយប្រឈមទៅនឹងការវាយប្រហារតាមអ៊ីនធឺណិត ដូចជា Eavesdropping (គឺជាទម្រង់នៃការវាយប្រហារតាមអ៊ីនធឺណិត ដែលអាចឱ្យពួក Hacker លុប ឬកែប្រែទិន្នន័យដែលត្រូវបានបញ្ជូនរវាងឧបករណ៍) ឬការវាយប្រហារបែប Man-in-the-middle (គឺជាទម្រង់នៃការវាយប្រហារមួយ ដែលពួក Hacker អាចចូលទៅក្នុងបណ្តាញទំនាក់ទំនងរវាងភាគីទាំងពីរដែលទុកចិត្តគ្នា ក្នុងគោលបំណងលួចស្តាប់ លួចទិន្នន័យ និងរំខានជាដើម)។ ដូច្នេះ វិធានការសុវត្ថិភាពអ៊ីនធឺណិត ដូចជា HTTPS ពិតជាមានសារៈសំខាន់ណាស់សម្រាប់ការធានាទិន្នន័យក្នុងអំឡុងពេល Transit និងរក្សាភាពត្រឹមត្រូវរបស់ទិន្នន័យ ដោយហេតុថាវិធានការនេះជួយការពារព័ត៌មានរសើបពីការចូលប្រើប្រាស់ដោយភាគីដែលគ្មានការអនុញ្ញាត។

● សុវត្ថិភាពអ៊ីនធឺណិតការពារសុវត្ថិភាពទិន្នន័យ និងឯកជនភាពទិន្នន័យ

នៅក្នុងទិដ្ឋភាពឌីជីថលនាពេលបច្ចុប្បន្ននេះ ការងារប្រចាំថ្ងៃជាច្រើនត្រូវបានសម្រេចនៅលើប្រព័ន្ធអ៊ីនធឺណិត ដែលនេះមានន័យថា ទិន្នន័យ និងព័ត៌មានរសើបជាច្រើនត្រូវបានចែករំលែកឥតឈប់ឈរនៅលើអ៊ីនធឺណិត។ ប្រព័ន្ធអ៊ីនធឺណិតអាចជាបណ្តាញដែលមិនមានសុវត្ថិភាពសម្រាប់ការផ្លាស់ប្តូរទិន្នន័យ ឬព័ត៌មាននានា និងជាកន្លែងដែលមានហានិភ័យខ្ពស់ពីការឈ្លានពានដោយពួក Hacker និងឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត ដូច្នេះ ការគិតគូរពីសុវត្ថិភាពអ៊ីនធឺណិតពិតជារឿងសំខាន់ដើម្បីធានាថាទិន្នន័យត្រូវបានការពារពីការគំរាមកំហែងពីខាងក្រៅ ដោយហេតុថាប្រសិនបើសុវត្ថិភាពអ៊ីនធឺណិតមិនត្រូវបានយកចិត្តទុកដាក់ អាចនាំឱ្យមានការរំលោភបំពានទាំងលើសុវត្ថិភាពទិន្នន័យ ឧ.ការចូលប្រើទិន្នន័យដែលបានរក្សាទុកដោយគ្មានការអនុញ្ញាត និងការបំពានឯកជនភាព ឧ.ការលេចចេញទិន្នន័យផ្ទាល់ខ្លួនអំឡុងពេលប្រតិបត្តិការអនឡាញជាដើម។

II. ធាតុផ្សំសំខាន់ៗនៃសុវត្ថិភាពទិន្នន័យ

សុវត្ថិភាពទិន្នន័យអាចត្រូវបានបែងចែកទៅជាធាតុសំខាន់ៗចំនួន ៤ រួមមាន **Data Confidentiality, Data Integrity, Data Authenticity** និង **Data Availability**។ ធាតុផ្សំ ដូចជា **Data Confidentiality** និង **Data Integrity** ជារឿយៗត្រូវបានចាត់ទុកថាជាធាតុផ្សំដ៏សំខាន់ក្នុងចំណោមធាតុផ្សំទាំងអស់ ប៉ុន្តែដើម្បីរក្សាសុវត្ថិភាពទិន្នន័យឱ្យបានប្រសើរ ធាតុផ្សំទាំង ៤ នេះគឺមិនអាចខ្វះធាតុណាមួយឡើយ។ ខាងក្រោមនេះគឺជាធាតុផ្សំសំខាន់ៗនៃសុវត្ថិភាពទិន្នន័យ៖

Data Confidentiality

ការអនុវត្តការរក្សាការសម្ងាត់ទិន្នន័យជាទូទៅរួមមានការធ្វើ Encryption ក្នុងពេលបញ្ជូនទិន្នន័យ, ការគ្រប់គ្រងលើម៉ាស៊ីនមេនិងឯកសារ និងការគ្រប់គ្រងលើឧបករណ៍របស់ក្រុមហ៊ុនដែលតម្រូវឱ្យមានការចូលប្រើប្រាស់ទិន្នន័យ។ ការរក្សាការសម្ងាត់ទិន្នន័យល្អអាចធានាថាអ្នកដែលអាចចូលប្រើទិន្នន័យគឺជាអ្នក ដែលនេះអាចកាត់បន្ថយពីការចូលប្រើប្រាស់ និងការផ្លាស់ប្តូរដោយគ្មានការអនុញ្ញាត។ ការអនុវត្តទាំងនេះបំពេញបន្ថែមគ្នាទៅវិញទៅមក ដើម្បីបង្កើតទិដ្ឋភាពទិន្នន័យសម្ងាត់បានប្រសើរ។

Data Integrity

Data Integrity អាចធានាបាននូវភាពត្រឹមត្រូវ ភាពស៊ីសង្វាក់ និងសុពលភាពនៃទិន្នន័យ ដើម្បីឱ្យទិន្នន័យរបស់អ្នកនៅតែមានភាពចាំបាច់។ ទិន្នន័យមិនមានភាពច្បាស់លាស់ ឬខុស មិនត្រឹមតែគ្មានប្រយោជន៍ប៉ុណ្ណោះទេ ប៉ុន្តែអាចប៉ះពាល់ដល់ការសម្រេចចិត្តអាជីវកម្ម ឬស្ថាប័នផងដែរ។ អាស្រ័យហេតុនេះ ការរក្សាបាននូវភាពត្រឹមត្រូវនៃទិន្នន័យ មិនត្រឹមតែជាទិដ្ឋភាពសំខាន់នៃសុវត្ថិភាពទិន្នន័យប៉ុណ្ណោះទេ ប៉ុន្តែព្រមទាំងបានធ្វើឱ្យទិន្នន័យមានមុខងារត្រឹមត្រូវ និងមានភាពច្បាស់លាស់ផងដែរ។

Data Authenticity

ស្រដៀងទៅនឹងគោលគំនិតនៃភាពត្រឹមត្រូវនៃទិន្នន័យ **Data Authenticity** ធានាថារាល់ទិន្នន័យទាំងអស់គឺមានភាពត្រឹមត្រូវ។ **Data Authenticity** និង **Data Integrity** គឺជាគោលការណ៍នៃសុវត្ថិភាពទិន្នន័យដែលដំណើរការជាមួយគ្នា ដើម្បីធានាថាទិន្នន័យមានភាពត្រឹមត្រូវ និងតម្រូវឱ្យមនុស្សតាមដាននូវអ្វីដែលបានកើតឡើងចំពោះទិន្នន័យទាំងនោះ។ **Data Authenticity** ជួយធានាសុវត្ថិភាពនៃប្រព័ន្ធទាំងមូលដោយគូសបញ្ជាក់ប្រភពដើមនៃទិន្នន័យ និងតាមដានកន្លែងដែលទិន្នន័យបញ្ជូនទៅ។ យើងអាចប្រៀបធៀប **Data Authenticity** ជាក្រដាសដែលកត់ត្រារាល់សកម្មភាពដែលបានអនុវត្តរបស់ទិន្នន័យ ដែលរួមបញ្ចូលទាំងការតាមដានថាតើអ្នកណា ឬអ្វីផ្សេងបានបង្កើតទិន្នន័យ, ពេលវេលាដែលទិន្នន័យត្រូវបានបង្កើត, ទិន្នន័យត្រូវបានបញ្ជូនទៅកាន់និងមកពីណា, របៀបដែលទិន្នន័យត្រូវបានផ្លាស់ប្តូររវាងទីតាំងផ្សេងៗ និងអ្នកណាបានចូលប្រើប្រាស់ទិន្នន័យ។

Data Availability

Data Availability គឺជាធាតុផ្សំមួយដែលគេមើលរំលងបំផុតនៃសុវត្ថិភាពទិន្នន័យ។ ការធានាថាទិន្នន័យដែលមាន និងអាចចូលប្រើបានគឺមានភាពចាំបាច់បំផុត ដោយហេតុថាបើទោះបីជាទិន្នន័យមានសុវត្ថិភាព និងត្រឹមត្រូវយ៉ាងណាក៏ដោយបើយើងគ្មានលទ្ធភាពក្នុងការប្រើប្រាស់ទិន្នន័យទាំងនោះគឺស្មើនឹងឥតប្រយោជន៍។ ទន្ទឹមនេះ យើងសង្កេតឃើញថា មានការគំរាមកំហែងជាច្រើនបានរារាំងចំពោះលទ្ធភាពក្នុងការប្រើប្រាស់ទិន្នន័យ ជាក់ស្តែង ការគំរាមកំហែងដ៏លេចធ្លោបំផុតមួយគឺ Ransomware

ដែលដកសិទ្ធិចូលប្រើប្រាស់ទិន្នន័យ និងរំខានដល់វដ្តអាជីវកម្ម និងស្ថាប័នទាំងមូល។ ការការពារដ៏ល្អបំផុតប្រឆាំងនឹងបញ្ហានេះ គឺការរក្សាការបម្រុងទុកទិន្នន័យឱ្យបានត្រឹមត្រូវ តាមរយៈការប្រើប្រាស់សេវាកម្ម ដែលជួយការពារទិន្នន័យប្រឆាំងនឹងការគំរាមកំហែងនានា។ បន្ថែមពីនេះ ប្រសិនបើ Datastore មួយចំនួនកំពុងត្រូវបានប្រើប្រាស់លើសពីសមត្ថភាព នេះក៏អាចនាំឱ្យមានការយឺតយ៉ាវ និងពិបាកក្នុងការចូលប្រើប្រាស់ទិន្នន័យផងដែរ។

III. បច្ចេកវិទ្យាដែលបានជះឥទ្ធិពលដល់សុវត្ថិភាពទិន្នន័យ

ក្នុងទិដ្ឋភាពឌីជីថលដែលកំពុងមានការវិវត្តនាពេលបច្ចុប្បន្ននេះ ទំហំ និងភាពស្មុគស្មាញនៃទិន្នន័យបានធ្វើឱ្យវិធានការសុវត្ថិភាពបែបប្រពៃណីមិនមានភាពគ្រប់គ្រាន់ឡើយ។ អាស្រ័យហេតុនេះ ស្ថាប័នជាច្រើនបានគិតគូរងាកទៅប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថលថ្មីៗ ដើម្បីបង្កើនសុវត្ថិភាពទិន្នន័យរបស់ស្ថាប័ន។ ខាងក្រោមនេះ នឹងបង្ហាញពីបច្ចេកវិទ្យាសំខាន់មួយចំនួនដែលមានសក្តានុពលដល់ការពង្រឹងសុវត្ថិភាពទិន្នន័យ៖

បច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត និងម៉ាស៊ីនសិក្សា

បច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត សំដៅលើសមត្ថភាពនៃប្រព័ន្ធកុំព្យូទ័រក្នុងការអនុវត្តកិច្ចការដែលជាធម្មតាត្រូវការភាពវៃឆ្លាតរបស់មនុស្ស ខណៈដែលម៉ាស៊ីនសិក្សា គឺផ្តោតលើការអភិវឌ្ឍនៃក្បួនដោះស្រាយ និងបច្ចេកទេសដែលអនុញ្ញាតឱ្យកុំព្យូទ័ររៀនពីទិន្នន័យ។ បច្ចេកវិទ្យាទាំងពីរនេះបានជះឥទ្ធិពលយ៉ាងខ្លាំងលើគ្រប់វិស័យ និងគ្រប់ផ្នែក ក្នុងនោះផ្នែកសុវត្ថិភាពទិន្នន័យក៏ដូចគ្នា ដោយបច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត និងម៉ាស៊ីនសិក្សាបានផ្តល់ឱ្យនូវបត់ថ្មីមួយនៅក្នុងផ្នែកសុវត្ថិភាពទិន្នន័យដែលបានអនុញ្ញាតឱ្យស្ថាប័នការពារទិន្នន័យសំខាន់របស់ពួកគេប្រកបដោយប្រសិទ្ធភាព។ បច្ចេកវិទ្យាទាំងពីរនេះបានដើរតួនាទីយ៉ាងសំខាន់ក្នុងការបង្កើនសុវត្ថិភាពទិន្នន័យ និងជះឥទ្ធិពលយ៉ាងខ្លាំងលើទិដ្ឋភាពផ្សេងៗនៃឥរិយាបថសុវត្ថិភាពរបស់ស្ថាប័នមួយ។ ជាក់ស្តែង ការកំណត់បាននូវការគំរាមកំហែងកម្រិតខ្ពស់បានទាន់ពេលវេលាពិតជារឿងសំខាន់ណាស់សម្រាប់ការការពារទិន្នន័យសំខាន់ ឬរសើបមិនឱ្យបាត់បង់។ ក្នុងនោះ បច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត និងម៉ាស៊ីនសិក្សាបានជះឥទ្ធិពលយ៉ាងខ្លាំងដល់ផ្នែកនេះ ដោយបានដើរតួនាទីចម្បងក្នុងការបង្កើនសុវត្ថិភាពទិន្នន័យ តាមរយៈសមត្ថភាពក្នុងវិភាគ និងស្វែងរកសកម្មភាពគំរាមកំហែងនានា។ បច្ចេកវិទ្យាទាំងពីរនេះអាចជួយកំណត់អត្តសញ្ញាណមិនប្រក្រតីដែលគេចចេញពីវិធានការសុវត្ថិភាព ហើយធ្វើការបញ្ជូនដំណឹងពីភាពមិនប្រក្រតី ដើម្បីឱ្យអ្នកគ្រប់គ្រងសុវត្ថិភាពទិន្នន័យអាចធ្វើការទប់ស្កាត់ទាន់ពេលវេលា ដែលនេះជួយឱ្យកំហុសផ្នែកសុវត្ថិភាពអាចត្រូវបានដោះស្រាយ មុនពេលដែលមានការបំពានទិន្នន័យកើតឡើង។ បន្ថែមពីនេះ បច្ចេកវិទ្យាទាំងពីរនេះក៏អាចគ្រប់គ្រងទិន្នន័យប្រភេទផ្សេងៗគ្នាជាច្រើន ដែលអាចជួយដល់ការវិភាគ និងទស្សន៍ទាយក្នុងពេលវេលាជាក់ស្តែងពីការគំរាមកំហែងតាមអ៊ីនធឺណិតដែលអាចកើតមាន ហើយធ្វើឱ្យប៉ះពាល់ដល់ការការពារសុវត្ថិភាពទិន្នន័យ។ ដូច្នេះ តាមរយៈការវិភាគទិន្នន័យដ៏ច្រើន

ក្នុងពេលវេលាជាក់ស្តែង បច្ចេកវិទ្យាទាំងនេះផ្តល់ឱ្យស្ថាប័ននូវសមត្ថភាពក្នុងការរកឃើញ និងកាត់បន្ថយការគំរាមកំហែងបានយ៉ាងឆាប់រហ័ស និងប្រកបដោយប្រសិទ្ធភាព ដែលជួយកាត់បន្ថយការខូចខាតដែលអាចកើតមាន។ ក្រៅពីនេះ បច្ចេកវិទ្យាទាំងពីរនេះក៏ដើរតួនាទីសំខាន់ក្នុងការជួយស្ថាប័នពង្រឹងការអនុលោមភាពតាមបទប្បញ្ញត្តិការការពារទិន្នន័យផងដែរ ដែលនេះផ្តល់ឱ្យនូវអត្ថប្រយោជន៍សំខាន់មួយដល់អ្នកប្រើប្រាស់ ដោយហេតុថាការអនុលោមភាពនេះគឺជាអាទិភាពចម្បងសម្រាប់ស្ថាប័ននៅពេលអនុវត្តវិធានការសុវត្ថិភាពនានា។ តាមរយៈសមត្ថភាពរបស់បច្ចេកវិទ្យាទាំងពីរក្នុងការធ្វើចំណាត់ថ្នាក់ទិន្នន័យដោយស្វ័យប្រវត្តិ, សមត្ថភាពក្នុងការអនុវត្តការគ្រប់គ្រងការចូលប្រើប្រាស់ និងការសម្របសម្រួលបច្ចេកទេសនៃការធ្វើអនាមិកទិន្នន័យ (Data Anonymization) បានជួយឱ្យស្ថាប័ននានាអាចឆ្លើយតប និងរក្សាការអនុលោមភាពតាមស្តង់ដាបទប្បញ្ញត្តិ ដូចជា General Data Protection Regulation (GDPR) និង The California Consumer Privacy Act (CCPA) ជាដើម ដែលនេះអាចជួយកាត់បន្ថយហានិភ័យនៃការពិន័យ, ការខូចខាតកេរ្តិ៍ឈ្មោះ និងការទទួលខុសត្រូវផ្នែកច្បាប់។

បច្ចេកវិទ្យាប្លុកឆេន (Blockchain)

បច្ចេកវិទ្យា Blockchain គឺប្រៀបបានទៅសៀវភៅកំណត់ហេតុមួយដែលកត់ត្រារាល់ប្រតិបត្តិការនានា ដើម្បីរក្សាទុកជាទិន្នន័យសំខាន់។ បច្ចេកវិទ្យានេះមានសក្តានុពលអាចប្រើសម្រាប់ការផ្ទេរហិរញ្ញវត្ថុ, ប្រតិបត្តិការទូទាត់ និងអាចដោះស្រាយផលវិបាកនានា។ ក្នុងនោះ បច្ចេកវិទ្យានេះក៏បានផ្តល់ឱ្យនូវសក្តានុពលដ៏សំខាន់សម្រាប់ការការពារសុវត្ថិភាពទិន្នន័យផងដែរ តាមរយៈការផ្តល់ឱ្យនូវសៀវភៅកត់ត្រាមួយដែលមានលក្ខណៈវិមជ្ឈការ និងមិនអាចផ្លាស់ប្តូរបានសម្រាប់ការកត់ត្រាប្រតិបត្តិការ និងការផ្លាស់ប្តូរទិន្នន័យ ដែលនេះធ្វើឱ្យកាន់តែពិបាកសម្រាប់អ្នកប្រើប្រាស់ក្នុងការផ្លាស់ប្តូរ ឬរំខាន (Tamper) ព័ត៌មានដោយពុំមានការអនុញ្ញាត។ បំណែកនីមួយៗនៃទិន្នន័យនៅលើបច្ចេកវិទ្យា Blockchain ត្រូវបាន Encrypted និងរក្សាទុកនៅក្នុង "ប្លុក" ដែលត្រូវបានភ្ជាប់ជាមួយគ្នានៅក្នុងខ្សែច្រវាក់មួយ ហើយនៅពេលដែលទិន្នន័យត្រូវបានកត់ត្រារួច វាស្ទើរតែមិនអាចទៅរួចទេក្នុងការកែប្រែប្លុកមួយដោយមិនផ្លាស់ប្តូររាល់ប្លុកជាបន្តបន្ទាប់។ បន្ថែមពីនេះទៀត សមត្ថភាពក្នុងការកត់ត្រាលក្ខណៈវិមជ្ឈការរបស់បច្ចេកវិទ្យានេះ ក៏ជួយលុបបំបាត់តម្រូវការសម្រាប់អាជ្ញាធរកណ្តាល មានន័យថា មិនមានអង្គភាពតែមួយដែលគ្រប់គ្រងព័ត៌មាននោះទេ ដែលនេះធ្វើឱ្យពួក Hacker កាន់តែពិបាកក្នុងការគ្រប់គ្រង ឬចូលប្រើប្រាស់ទិន្នន័យ។ ការណ៍នេះ កម្រិតនៃភាពមិនប្រែប្រួល និងកំណត់ត្រាលក្ខណៈវិមជ្ឈការនេះ ធានាបាននូវភាពត្រឹមត្រូវនៃកំណត់ត្រាឌីជីថល, បង្កើនប្រសិទ្ធភាពទិន្នន័យ និងជាពិសេសបន្ថែមវិធានការសុវត្ថិភាពប្រកបដោយប្រសិទ្ធភាពដល់យុទ្ធសាស្ត្រសុវត្ថិភាពរបស់ស្ថាប័នដែលប្រើប្រាស់ផងដែរ។

Security Orchestration, Automation and Response (SOAR)

SOAR សំដៅលើដំណោះស្រាយ Software ដែលអាចឱ្យអ្នកគ្រប់គ្រងសុវត្ថិភាពទិន្នន័យអាចរួមបញ្ចូល និងសម្របសម្រួលឧបករណ៍សុវត្ថិភាពជាច់ដោយឡែក, ធ្វើកិច្ចការដដែលៗដោយស្វ័យប្រវត្តិ និងជួយសម្រួលលំហូរការងារពាក់ព័ន្ធនឹងការឆ្លើយតបនឹងការគំរាមកំហែង ដែលទាំងអស់នេះមានសារៈសំខាន់សម្រាប់ការការពារ ឬកាត់បន្ថយការខូចខាតពីការវាយប្រហារតាមអ៊ីនធឺណិត។ បច្ចេកវិទ្យានេះអនុញ្ញាតឱ្យរកឃើញភាពមិនប្រក្រតី និងសកម្មភាពគួរឱ្យសង្ស័យបានលឿនជាងមុន ក៏ដូចជាធ្វើស្វ័យប្រវត្តិកម្មនូវការឆ្លើយតបដែលបានកំណត់ជាមុន ដូចជា ការដាក់ប្រព័ន្ធដែលរងផលប៉ះពាល់ឱ្យនៅដាច់ដោយឡែក ឬទប់ស្កាត់ IPs ដែលគួរឱ្យសង្ស័យ ដោយមិនរង់ចាំការអន្តរាគមន៍ពីមនុស្ស ដែលនេះជួយកាត់បន្ថយពេលវេលាឆ្លើយតបទៅនឹងការគំរាមកំហែងនានា ឬក៏អាចទប់ស្កាត់មុនពេលការគំរាមកំហែងទាំងនោះបណ្តាលឱ្យមានការខាតបង់ធ្ងន់ធ្ងរ។ បន្ថែមពីនេះ បច្ចេកវិទ្យានេះក៏ជួយសម្រួលដល់ការរួមបញ្ចូល និងការសម្របសម្រួលឧបករណ៍ និងដំណើរការសុវត្ថិភាពផ្សេងៗដោយធានាបាននូវវិធីសាស្ត្រស្របគ្នាក្នុងការគ្រប់គ្រងការគំរាមកំហែងនៅទូទាំងហេដ្ឋារចនាសម្ព័ន្ធរបស់ស្ថាប័នមួយ។ ក្រៅពីនេះ បច្ចេកវិទ្យានេះក៏ជួយធានាថាគោលការណ៍សុវត្ថិភាពត្រូវបានអនុវត្តជាប់លាប់នៅទូទាំងប្រព័ន្ធទាំងអស់ ធ្វើអោយប្រសើរឡើងនូវពេលវេលាឆ្លើយតបទៅនឹងឧប្បត្តិហេតុ និងធ្វើឱ្យការអនុលោមតាមតម្រូវការបទប្បញ្ញត្តិកាន់តែងាយស្រួលផងដែរ។

Multi-factor Authentication

MFA គឺជាបច្ចេកវិទ្យាសុវត្ថិភាពមួយ ដែលផ្តល់ឱ្យនូវស្រទាប់សុវត្ថិភាពបន្ថែម តាមរយៈការតម្រូវឱ្យអ្នកប្រើប្រាស់ផ្តល់ឱ្យនូវវិធីសាស្ត្រផ្ទៀងផ្ទាត់ពីរ ឬច្រើន ដើម្បីផ្ទៀងផ្ទាត់អត្តសញ្ញាណរបស់អ្នកប្រើប្រាស់ មុនពេលពួកគេអាចចូលប្រើប្រាស់ ដូចជា គណនីអនឡាញ ឬកម្មវិធីនានា។ ការពង្រឹងសុវត្ថិភាពគឺជាអត្ថប្រយោជន៍ចម្បងមួយនៃបច្ចេកវិទ្យាសុវត្ថិភាពនេះ។ ការប្រើប្រាស់ការផ្ទៀងផ្ទាត់ច្រើនស្រទាប់អាចជួយកាត់បន្ថយហានិភ័យនៃការចូលប្រើដោយគ្មានការអនុញ្ញាត, ជួយការពារការវាយប្រហារដោយបន្លំ និងការបំពានដែលទាក់ទងនឹងពាក្យសម្ងាត់ ដែលបានកើតឡើងកាន់តែខ្លាំងឡើងនៅក្នុងទិដ្ឋភាពឌីជីថលនាពេលបច្ចុប្បន្ននេះ។ ការណ៍នេះ បង្ហាញថាការពង្រឹងសុវត្ថិភាពគឺជាទិដ្ឋភាពសំខាន់នៃ MFA ដែលធ្វើឱ្យបច្ចេកវិទ្យានេះបានក្លាយជាឧបករណ៍សំខាន់សម្រាប់ការការពារប្រឆាំងនឹងការវាយប្រហារតាមអ៊ីនធឺណិត និងការបំពានទិន្នន័យ បើទោះបីជាពួក Hacker មានពាក្យសម្ងាត់របស់អ្នកក៏ដោយ។ ក្រៅពីការពង្រឹងសុវត្ថិភាព MFA អាចជួយកាត់បន្ថយតម្រូវការសម្រាប់ការកំណត់ពាក្យសម្ងាត់ឡើងវិញ និងជួយឱ្យស្ថាប័នអាចជៀសវាងពីការជាកពិន័យ ការចំណាយលើវិវាទ និងការបាត់បង់កេរ្តិ៍ឈ្មោះ ដែលបណ្តាលមកពីការបំពានទិន្នន័យ។ ដូច្នេះ ក្រៅពីការពង្រឹងសុវត្ថិភាព MFA ក៏ជួយកាត់បន្ថយការចំណាយរបស់ស្ថាប័ន ឬអាជីវកម្មដែលប្រើប្រាស់បច្ចេកវិទ្យាសុវត្ថិភាពនេះផងដែរ។

IV. អត្ថប្រយោជន៍នៃសុវត្ថិភាពទិន្នន័យ

ការប្រមូល រក្សាទុក វិភាគ និងប្រើប្រាស់ទិន្នន័យបានក្លាយជាភាពចាំបាច់មួយសម្រាប់ស្ថាប័ន និងអាជីវកម្មជាច្រើន ដើម្បីជំរុញដំណើរការសម្រេចចិត្តរបស់ពួកគេ និងរក្សាបាននូវភាពប្រកួតប្រជែងនៅក្នុងទីផ្សារផងដែរ។ ទោះជាយ៉ាងណាក៏ដោយ ជាមួយនឹងការកើនឡើងនៃការពឹងផ្អែកទៅលើទិន្នន័យនេះ តម្រូវការ សម្រាប់វិធានការសុវត្ថិភាពទិន្នន័យដ៏រឹងមាំ ដើម្បីការពារព័ត៌មានដ៏មានតម្លៃ និងរសើបពីការគំរាមកំហែងទាំងខាងក្នុង និងខាងក្រៅពិតជាមានភាពចាំបាច់។ ដូច្នេះ តើការដាក់ចេញនូវវិធានការសុវត្ថិភាពទិន្នន័យដ៏ត្រឹមត្រូវបានផ្តល់ឱ្យនូវអត្ថប្រយោជន៍អ្វីខ្លះ?

ការពារការបាត់បង់ ឬការបំពានលើទិន្នន័យសំខាន់ ឬរសើប

អត្ថប្រយោជន៍សំខាន់ទីមួយនៃការដាក់ចេញវិធានការសុវត្ថិភាពទិន្នន័យ គឺការផ្តល់ឱ្យនូវការការពារទិន្នន័យសំខាន់ ឬរសើបរបស់ស្ថាប័ន និងអាជីវកម្ម។ សុវត្ថិភាពទិន្នន័យដើរតួនាទីយ៉ាងសំខាន់ក្នុងការការពារព័ត៌មានរសើបដោយអនុវត្តវិធានការផ្សេងៗ ដើម្បីការពារការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត ការលួច ឬការខូចខាតទិន្នន័យ។ តាមរយៈការធ្វើ Encryption និងការគ្រប់គ្រងការចូលប្រើជាដើម សុវត្ថិភាពទិន្នន័យធានាថាមានតែបុគ្គល ឬប្រព័ន្ធដែលមានការអនុញ្ញាតប៉ុណ្ណោះដែលអាចចូលប្រើ ឬកែប្រែទិន្នន័យរសើបបាន។ វិធានការសុវត្ថិភាពទិន្នន័យក៏រួមបញ្ចូលផងដែរ នូវសកម្មភាពត្រួតពិនិត្យ និងសវនកម្ម ដើម្បីរកឱ្យឃើញនូវអាកប្បកិរិយាមិនប្រក្រតី ឬគួរឱ្យសង្ស័យណាមួយ ដោយជួយកំណត់អត្តសញ្ញាណការបំពានដែលអាចកើតមានមុនពេលទិន្នន័យសំខាន់ ឬរសើបត្រូវបានបំពាន។

ការរក្សាទំនុកចិត្តរបស់អតិថិជន និងការពារកេរ្តិ៍ឈ្មោះរបស់ស្ថាប័ន

ការបំពាន ឬការបាត់បង់ទិន្នន័យណាមួយអាចធ្វើឱ្យស្ថាប័ន និងអាជីវកម្មមានការខូចខាតកេរ្តិ៍ឈ្មោះយ៉ាងខ្លាំង ក៏ដូចជាធ្វើឱ្យទំនុកចិត្ត ឬភាពជឿជាក់របស់អតិថិជនមកលើស្ថាប័នត្រូវបានកាត់បន្ថយ។ អាស្រ័យហេតុនេះ ការអនុវត្តវិធានការសុវត្ថិភាពពិតជារឿងមួយសំខាន់សម្រាប់ស្ថាប័ន និងអាជីវកម្មក្នុងការគិតគូរ ដោយហេតុថា វិធានការសុវត្ថិភាពអាចជួយរក្សាទំនុកចិត្ត និងភាពជឿជាក់របស់អតិថិជន តាមរយៈការការពារទិន្នន័យឯកជនរបស់ពួកគេពីការចូលប្រើ ការលួច ឬការបាត់បង់ដោយគ្មានការអនុញ្ញាត។ បន្ថែមពីនេះ ការអនុវត្តវិធានការសុវត្ថិភាពទិន្នន័យក៏បង្ហាញពីការប្តេជ្ញាចិត្តរបស់ស្ថាប័ន និងអាជីវកម្ម ក្នុងការការពារឯកជនភាព និងព័ត៌មានរសើបរបស់អតិថិជនរបស់ខ្លួន ដែលនេះអាចបង្កើនកេរ្តិ៍ឈ្មោះ និងទាក់ទាញអតិថិជនថ្មីផងដែរ។

ការផ្តល់ឱ្យនូវឧត្តមភាពប្រកួតប្រជែង

វិធានការសុវត្ថិភាពទិន្នន័យមិនត្រឹមតែជួយស្ថាប័ន និងអាជីវកម្មក្នុងការរក្សាទំនុកចិត្តរបស់អតិថិជន និងការពារកេរ្តិ៍ឈ្មោះរបស់ស្ថាប័នប៉ុណ្ណោះទេ ប៉ុន្តែអត្ថប្រយោជន៍ទាំងនេះក៏ផ្តល់ឱ្យស្ថាប័ន និងអាជីវកម្មនូវឧត្តមភាពប្រកួតប្រជែងផងដែរ។ ស្ថាប័ន និងអាជីវកម្មដែលគិតគូរក្នុងការអនុវត្តវិធានការសុវត្ថិភាពទិន្នន័យអាចជួយឱ្យពួកគេមានប្រៀប និងលេចធ្លោជាងដៃគូប្រកួតប្រជែងរបស់ពួកគេដែលមិនបានអនុវត្តវិធានការសុវត្ថិភាពរឹងមាំ។ ឧត្តមភាពប្រកួតប្រជែងនេះនឹងជួយឱ្យស្ថាប័ន និងអាជីវកម្ម អាចរក្សាទំនាក់ទំនងល្អជាមួយអតិថិជន, ទាក់ទាញអតិថិជនថ្មីកាន់តែច្រើន និងអាចរក្សាភាពប្រកួតប្រជែងរបស់ខ្លួននៅក្នុងទីផ្សារផងដែរ។

ការជួយស្តាប័ន និងអាជីវកម្មជៀសវាងការចំណាយបន្ថែម

ការបំពានទិន្នន័យបានក្លាយជាបញ្ហាប្រឈមមួយ ដែលបានធ្វើឱ្យស្ថាប័ន និងអាជីវកម្មជាច្រើនរងការខាតបង់ ជាក់ស្តែង យោងតាមទិន្នន័យរបស់ Statista បានបង្ហាញថា នៅក្នុងឆ្នាំ២០២៤ ការចំណាយជាមធ្យមដែលបណ្តាលមកពីការបំពានទិន្នន័យនៅកម្រិតសកលមានចំនួនប្រមាណ ៤,៨៨លានដុល្លារ។ បញ្ហាប្រឈមនេះបានឆ្លុះបញ្ចាំងពីអត្ថប្រយោជន៍សំខាន់មួយទៀតរបស់សុវត្ថិភាពទិន្នន័យក្នុងការដោះស្រាយបញ្ហានេះ ដែលជាការជួយស្តាប័ន និងអាជីវកម្មជៀសវាងការចំណាយបន្ថែម។ តាមរយៈការអនុវត្តវិធានការសុវត្ថិភាពទិន្នន័យ ស្ថាប័ននានាអាចអនុលោមភាពតាមបទប្បញ្ញត្តិសុវត្ថិភាពទិន្នន័យបានត្រឹមត្រូវ ដែលអាចជួយឱ្យស្ថាប័នមិនខាតបង់លើចំណាយបន្ថែម ដូចជា ការផាកពិន័យ ឬការចំណាយលើផ្លូវច្បាប់ និងការចំណាយបណ្តាលមកពីការខូចខាតកេរ្តិ៍ឈ្មោះ និងការបាត់បង់អតិថិជនជាដើម។

V. ករណីសិក្សា

ការពង្រឹងសុវត្ថិភាពទិន្នន័យនៅប្រទេសកម្ពុជា

និន្នាការសកលនៃបដិវត្តន៍ឧស្សាហកម្មទី ៤ បន្ថែមដោយការរីករាលដាលនៃជំងឺកូវីដ-១៩ បានជំរុញឱ្យកម្ពុជាពន្លឿនការអភិវឌ្ឍសេដ្ឋកិច្ច និងសង្គមដោយប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថល ដែលជាឃ្នាស់នៃការជំរុញប្រភពកំណើនថ្មី ដើម្បីសម្រេចបានចក្ខុវិស័យប្រែក្លាយកម្ពុជាទៅជាប្រទេសចំណូលមធ្យមកម្រិតខ្ពស់នៅឆ្នាំ២០៣០ និងជាប្រទេសចំណូលខ្ពស់នៅឆ្នាំ២០៥០។ ក្នុងន័យនេះ **ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ចនិងសង្គមឌីជីថលកម្ពុជា ២០២១-២០៣៥** ត្រូវបានរៀបចំឡើង

ដើម្បីឆ្លើយតបនឹងដំណើរការនៃឌីជីថលភាវូបនីយកម្មនេះ។ ទោះជាយ៉ាងណាក៏ដោយ នៅក្នុងដំណើរការនៃការជំរុញបរិវត្តកម្មឌីជីថលនេះ កម្ពុជាក៏បានប្រឈមមុខនឹងបញ្ហាប្រឈមមួយចំនួន រួមមាន បទល្មើសពាក់ព័ន្ធនឹងសន្តិសុខឌីជីថល ការការពារទិន្នន័យបុគ្គល សុវត្ថិភាពទិន្នន័យ ឧក្រិដ្ឋកម្មឆ្លងដែន និងការកេងប្រវ័ញ្ចនិងរំលោភបំពានផ្លូវភេទលើកុមារនិងស្ត្រីតាមអនឡាញ។ ជាការឆ្លើយតប រដ្ឋាភិបាលកម្ពុជាបានដាក់ចេញជាសេចក្តីព្រាងច្បាប់នានា ដើម្បីដោះស្រាយបញ្ហាប្រឈមឌីជីថលនានានៅក្នុងយុគសម័យឌីជីថលនេះ។

▶ កិច្ចខិតខំប្រឹងប្រែងរបស់រាជរដ្ឋាភិបាល និងភាគីពាក់ព័ន្ធ ក្នុងការពង្រឹងសុវត្ថិភាពទិន្នន័យនៅកម្ពុជា

រដ្ឋាភិបាលកម្ពុជាបានព្យាយាម និងយកចិត្តទុកដាក់យ៉ាងខ្លាំងក្នុងការពង្រឹងសុវត្ថិភាពទិន្នន័យនៅកម្ពុជា ជាក់ស្តែង នៅក្នុងឆ្នាំ២០១២ រាជរដ្ឋាភិបាលបានប្រកាសពីដំណើរការនៃការតាក់តែងច្បាប់ស្តីពីបទល្មើសតាមអ៊ីនធឺណិត ដោយសេចក្តីព្រាងច្បាប់នេះបានឆ្លងកាត់កិច្ចប្រជុំ និងពិគ្រោះយោបល់ជាមួយអ្នកជំនាញជាច្រើនលើកជាច្រើនសារ ដើម្បីឱ្យសេចក្តីព្រាងច្បាប់នេះមានភាពសុក្រឹតគោរពតាមស្តង់ដាអន្តរជាតិ និងដើម្បីឱ្យការប្រើប្រាស់បច្ចេកវិទ្យានៅកម្ពុជាកាន់តែមានសុវត្ថិភាព ហើយគ្រោងនឹងសម្រេចការតាក់តែងច្បាប់នេះក្នុងពេលឆាប់ៗនេះ។ បន្ថែមពីនេះទៀត នៅក្នុង **ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ចនិងសង្គមឌីជីថលកម្ពុជា ២០២១-២០៣៥** រាជរដ្ឋាភិបាលក៏បានបង្ហាញពីការប្តេជ្ញាចិត្តយ៉ាងមុតមាំក្នុងការប្រយុទ្ធប្រឆាំងនឹងការវាយប្រហារតាមអ៊ីនធឺណិតតាមរយៈការបង្កើតនូវ **«គណៈកម្មាធិការសន្តិសុខឌីជីថល»** ដែលអនុក្រឹត្យ ស្តីពី ការរៀបចំនិងការប្រព្រឹត្តទៅរបស់គណៈកម្មាធិការសន្តិសុខឌីជីថល ត្រូវបានដាក់ចេញកាលពីថ្ងៃទី០១ ខែមីនា ឆ្នាំ២០២៤។ ការបង្កើតគណៈកម្មាធិការសន្តិសុខឌីជីថលនេះធ្វើឡើងក្នុងគោលបំណងធានាប្រសិទ្ធភាពនិងស័ក្តិសិទ្ធិភាពនៃការបំពេញមុខងារ ដឹកនាំ សម្របសម្រួល និងជំរុញការគ្រប់គ្រងសន្តិសុខឌីជីថលដើម្បីការពារអត្ថប្រយោជន៍របស់គ្រប់តួអង្គសង្គមទប់ទល់នឹងការវាយប្រហារគ្រប់រូបភាព ឆ្លើយតបគ្រប់ផ្នែកទាំងបច្ចេកទេសនិងកម្លាំងពាក់ព័ន្ធនឹងការធានានិងការពារសន្តិសុខឌីជីថល។ លើសពីនេះ រដ្ឋាភិបាលកម្ពុជាក៏កំពុងរៀបចំសេចក្តីព្រាងច្បាប់ និងដាក់ចេញអនុក្រឹតនានាផងដែរ សំដៅលើកកម្ពស់វិធានការសុវត្ថិភាពទិន្នន័យ ដូចជា សេចក្តីព្រាងច្បាប់ការពារទិន្នន័យផ្ទាល់ខ្លួន, សេចក្តីព្រាងច្បាប់ស្តីពីសន្តិសុខសាយប័រ និងអនុក្រឹត ស្តីពី ការគ្រប់គ្រង ការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គលជាដើម។

ក្រៅពីនេះ វិស័យឯកជន ជាពិសេសស្ថាប័នហិរញ្ញវត្ថុ ក៏ជាកត្តាជំរុញសំខាន់មួយក្នុងការធ្វើឱ្យប្រសើរឡើងនូវសុវត្ថិភាពទិន្នន័យនៅក្នុងប្រទេសកម្ពុជា។ ជាក់ស្តែង ក្រុមហ៊ុន វីសា ដែលជាក្រុមហ៊ុនបច្ចេកវិទ្យាទូទាត់សាច់ប្រាក់តាមប្រព័ន្ធឌីជីថលដែលឈានមុខគេនៅក្នុងពិភពលោក ក៏បានដាក់ចេញនូវផែនទីសុវត្ថិភាពសម្រាប់ប្រទេសកម្ពុជាដោយបានគូសបញ្ជាក់នូវវិធីសាស្ត្រដ៏រឹងមាំសម្រាប់ពង្រឹងសុវត្ថិភាពក្នុងការទូទាត់នៅប្រទេសកម្ពុជា។ នៅក្នុងគំនិតផ្តួចផ្តើមលើសុវត្ថិភាពទាំងនោះ រួមមាន

ទិន្នន័យត្រូវបានការពារដោយមិនងាយក្លែងបន្លំក្នុងពេលធ្វើប្រតិបត្តិការ, ការពារទិន្នន័យ ដោយអនុវត្តគោលការណ៍សុវត្ថិភាពដើម្បីការពារទិន្នន័យផ្ទាល់ខ្លួន ក៏ដូចជាព័ត៌មានលម្អិតអំពីគណនី, បំពាក់ទិន្នន័យ ដោយកំណត់អត្តសញ្ញាណនៃការក្លែងបន្លំដ៏គួរឱ្យកត់សម្គាល់ណាមួយ មុនពេលមានបញ្ហាកើតឡើង និងបង្កើនទំនុកចិត្តក្នុងការអនុម័តលើប្រតិបត្តិការដែលត្រឹមត្រូវ។

▶ បញ្ហាប្រឈម និងអនាគតនៃសុវត្ថិភាពទិន្នន័យនៅកម្ពុជា

បើទោះបីជាមានការខិតខំប្រឹងប្រែងខាងលើក៏ដោយ ប្រទេសកម្ពុជានៅតែជួបប្រទះបញ្ហាប្រឈមមួយចំនួននៅក្នុងដំណើរការពង្រឹងសុវត្ថិភាពទិន្នន័យ ជាក់ស្តែងដូចជា បញ្ហាកង្វះការយល់ដឹងច្បាស់ពីសារៈសំខាន់នៃសុវត្ថិភាពទិន្នន័យ និងខ្វះខាតអ្នកជំនាញ, ដែនកំណត់ហេដ្ឋារចនាសម្ព័ន្ធឌីជីថលនៅមានកម្រិត និងចំនួននៃការវាយប្រហារតាមអ៊ីនធឺណិត និងការរំលោភបំពានទិន្នន័យស្ថិតនៅកម្រិតមួយដែលជាបញ្ហាកង្វល់នៅឡើយ ប៉ុន្តែកម្ពុជាក៏នៅតែមានសក្តានុពលក្នុងការចាប់យកឱកាសក្នុងការពង្រឹងសុវត្ថិភាពទិន្នន័យ។ តាមរយៈការប្តេជ្ញាចិត្តសហការជាមួយនឹងដៃគូក្នុងស្រុក និងក្រៅតំបន់ ដើម្បីសិក្សាពីការអនុវត្តល្អៗកន្លងមក ដើម្បីបញ្ចូលក្នុងគោលនយោបាយ និងពង្រឹងការអនុវត្តវិធានការសុវត្ថិភាពទិន្នន័យនៅកម្ពុជា និងការឈានទៅសម្រេចបានការតាក់តែងច្បាប់ដែលបានព្រាងកន្លងមក កម្ពុជានឹងសម្រេចបានការអភិវឌ្ឍលើផ្នែកសុវត្ថិភាពទិន្នន័យ ហើយការអនុវត្តវិធានការសុវត្ថិភាពទិន្នន័យនឹងមានកំណើននាពេលអនាគតផងដែរ។

▶▶ ការបំពានទិន្នន័យ Equifax៖ ការបរាជ័យនៃសន្តិសុខសាយប័រ

ការបំពានទិន្នន័យ Equifax ឆ្នាំ២០១៧ គឺជាឧប្បត្តិហេតុសន្តិសុខសាយប័រដ៏សំខាន់បំផុតមួយនៅក្នុងប្រវត្តិសាស្ត្រទំនើប ដែលបានបង្ហាញព័ត៌មានផ្ទាល់ខ្លួនរបស់បុគ្គលប្រមាណ **១៤៧លាននាក់**។ **Equifax** គឺជាភ្នាក់ងាររាយការណ៍ឥណទានធំមួយក្នុងចំណោមភ្នាក់ងាររាយការណ៍ឥណទានធំៗទាំង ៣ នៅសហរដ្ឋអាម៉េរិក ដោយ Equifax បានរក្សាទុកទិន្នន័យរសើបយ៉ាងច្រើន រួមទាំងលេខសន្តិសុខសង្គម ថ្ងៃខែឆ្នាំកំណើត អាសយដ្ឋាន លេខប័ណ្ណបើកបរ និងព័ត៌មានលម្អិតអំពីប័ណ្ណឥណទាន។ ការបំពាននេះមិនត្រឹមតែប៉ះពាល់ដល់ឯកជនភាព និងសុវត្ថិភាពរបស់មនុស្សរាប់លាននាក់ប៉ុណ្ណោះទេ ប៉ុន្តែថែមទាំងបង្ហាញពីគុណវិបត្តិសំខាន់ៗនៅក្នុងការអនុវត្តសុវត្ថិភាពតាមអ៊ីនធឺណិត និងការគ្រប់គ្រងរបស់ Equifax ផងដែរ។

ការបំពានទិន្នន័យនេះបានកើតឡើងនៅចន្លោះខែឧសភា និងខែកក្កដា ឆ្នាំ២០១៧ ប៉ុន្តែមិនត្រូវបានបង្ហាញជាសាធារណៈនោះទេ រហូតដល់ខែកញ្ញាទើបមានការបែកធ្លាយនូវព័ត៌មាន។ ទោះបីជា Patch សម្រាប់ការការពារនេះមានតាំងពីខែមីនា ឆ្នាំ២០១៧ ក៏ដោយ ប៉ុន្តែ Equifax បានបរាជ័យក្នុងការអនុវត្ត Patch នេះទៅក្នុងប្រព័ន្ធរបស់ខ្លួន។ ការបរាជ័យនេះបានអនុញ្ញាតឱ្យឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតជ្រៀតចូលទៅក្នុងបណ្តាញរបស់ក្រុមហ៊ុន និងទាញយកនូវទិន្នន័យរសើបក្នុងរយៈពេលជាច្រើនខែ។ បន្ថែមពីនេះ ការបំពាននេះគឺពុំអាចរកឃើញបាននោះទេ ដោយហេតុថាការត្រួតពិនិត្យមិនមានភាពគ្រប់គ្រាន់ និងវិធីសាស្ត្រសុវត្ថិភាពមានភាពហួសសម័យ ដែលនេះបានបង្ហាញពីកង្វះការត្រៀមខ្លួន និងការត្រួតពិនិត្យរបស់ក្រុមហ៊ុនមួយនេះ។ ផលប៉ះពាល់នៃការរំលោភបំពាននេះគឺមានសភាពធ្ងន់ធ្ងរខ្លាំង ដែល Equifax ត្រូវប្រឈមមុខនឹងប្រតិកម្មជាសាធារណៈយ៉ាងធ្ងន់ធ្ងរ រួមទាំងការស៊ើបអង្កេតបទប្បញ្ញត្តិ និងចំណាត់ការផ្លូវច្បាប់។ កេរ្តិ៍ឈ្មោះរបស់ក្រុមហ៊ុនត្រូវបានខូចខាត ហើយតម្លៃភាគហ៊ុនក៏បានធ្លាក់ចុះផងដែរ។ នៅឆ្នាំ២០១៩ Equifax បានយល់ព្រមលើការទូទាត់សំណងរហូតដល់ **៤២៥លានដុល្លារ** ជាមួយ Federal Trade Commission, The Consumer Financial Protection Bureau និង 50 U.S. states and territories។ ដំណោះស្រាយនេះរួមបញ្ចូលសំណងសម្រាប់បុគ្គល ដែលរងផលប៉ះពាល់ និងការជាកពិន័យដើម្បីកែលម្អវិធានការសន្តិសុខសាយប័រ។ ទោះជាយ៉ាងណាក៏ដោយ ការចំណាយផ្នែកហិរញ្ញវត្ថុ និងកេរ្តិ៍ឈ្មោះរបស់ក្រុមហ៊ុនគ្រាន់តែជាផ្នែកមួយនៃបញ្ហានេះប៉ុណ្ណោះ ដោយការបំពាននេះក៏បានធ្វើឱ្យមនុស្សរាប់លាននាក់ប្រឈមនឹងហានិភ័យនៃការលួចអត្តសញ្ញាណ និងការក្លែងបន្លំហិរញ្ញវត្ថុ ជាមួយនឹងផលប៉ះពាល់រយៈពេលវែងសម្រាប់សុវត្ថិភាពហិរញ្ញវត្ថុរបស់ពួកគេផងដែរ។ ជាមួយគ្នានេះដែរ ក្រុមហ៊ុនបានពន្យារពេលជូនដំណឹងដល់សាធារណជនរយៈពេល ៦ សប្តាហ៍ ក្នុងអំឡុងពេលនោះ នាយកប្រតិបត្តិជាច្រើននាក់បានលក់ភាគហ៊ុន ដែលបង្កឱ្យមានការសង្ស័យនៃការជួញដូរនៅក្នុងក្រុមហ៊ុន។ កង្វះតម្លាភាពនេះ បានបំផ្លាញទំនុកចិត្តលើក្រុមហ៊ុនបន្ថែមទៀត និងបានគូសបញ្ជាក់អំពីសារៈសំខាន់នៃការទំនាក់ទំនងទាន់ពេលវេលា និងភាពស្មោះត្រង់បន្ទាប់ពីមានការរំលោភបំពានទិន្នន័យ។ ការខកខានរបស់ Equifax ក្នុងការធ្វើសកម្មភាពឱ្យបានឆាប់រហ័ស និងប្រកបដោយទំនួលខុសត្រូវបានបង្ហាញពីការខ្វះទំនួលខុសត្រូវ និងការមិនយកចិត្តទុកដាក់ចំពោះផលប៉ះពាល់លើអតិថិជនរបស់ខ្លួន។

▶ មេរៀនអំពីឧប្បត្តិហេតុសន្តិសុខសាយប័រនេះ

ការបំពានទិន្នន័យ Equifax បានបង្ហាញមេរៀនសំខាន់ៗជាច្រើនដែលយើងក្នុងនាមជាបុគ្គល ឬស្ថាប័នគួរយកចិត្តទុកដាក់ស្វែងយល់ ជាពិសេសលើការការពារទិន្នន័យផ្ទាល់ខ្លួន និងរបស់អតិថិជន។ ហេតុការណ៍នេះបានគូសបញ្ជាក់ពីភាពងាយរងគ្រោះដែលមាននៅក្នុងការផ្ទុកព័ត៌មានរសើបផ្ទាល់ខ្លួន និងតម្រូវការសម្រាប់ក្រុមហ៊ុននានាក្នុងការអនុវត្តវិធីសាស្ត្រសុវត្ថិភាពទិន្នន័យដែលមានភាពច្បាស់លាស់។ ការបំពានក៏បានជំរុញឱ្យមានការពិភាក្សាអំពីការគ្រប់គ្រងរបស់ភ្នាក់ងាររាយការណ៍ឥណទាន និងភាពចាំបាច់សម្រាប់តម្លាភាព និងគណនេយ្យភាពក្នុងការដោះស្រាយទិន្នន័យអ្នកប្រើប្រាស់ផងដែរ។

ខាងក្រោមនេះជា ៤ ចំណុចសំខាន់ៗដែលយើងអាចសិក្សាបានពីឧប្បត្តិហេតុបំពានទិន្នន័យ Equifax៖

- ទី១. ហេតុការណ៍នេះបានគូសបញ្ជាក់ពីសារៈសំខាន់នៃការអនុវត្តការធ្វើបច្ចុប្បន្នភាពកម្មវិធី និងការអនុវត្ត Patches ភ្លាមៗ។ ការបំពានអាចត្រូវបានការពារប្រសិនបើ Equifax បានដោះស្រាយបញ្ហារបស់ Apache Struts នៅពេលដែលការជួសជុលត្រូវបានចេញផ្សាយ។
- ទី២. ការបំពានបង្ហាញពីហានិភ័យ ដែលទាក់ទងនឹងការរក្សាទុកព័ត៌មានរសើបផ្ទាល់ខ្លួនច្រើននៅលើប្រព័ន្ធអ៊ីនធឺណិត ឬក្រុមហ៊ុន។ ស្ថាប័នត្រូវតែអនុវត្តការធ្វើ Encryption ឱ្យបានរឹងមាំ, គ្រប់គ្រងការចូលប្រើប្រាស់ និងមានប្រព័ន្ធត្រួតពិនិត្យដើម្បីការពារទិន្នន័យ។ បន្ថែមពីនេះ ការធ្វើសវនកម្មសុវត្ថិភាពជាប្រចាំ និងការបណ្តុះបណ្តាលបុគ្គលិកក៏មានសារៈសំខាន់ផងដែរក្នុងការទប់ស្កាត់ និងស្វែងរកការបំពាន។
- ទី៣. តម្លាភាព និងការប្រាស្រ័យទាក់ទងទាន់ពេលវេលាគឺមានសារៈសំខាន់បំផុត។ ការពន្យារពេលរបស់ Equifax ក្នុងការជូនដំណឹងដល់សាធារណជនបានធ្វើឱ្យខូចខាតដល់កេរ្តិ៍ឈ្មោះរបស់ខ្លួន។ ក្រុមហ៊ុនត្រូវតែមានផែនការឆ្លើយតបការរំលោភបំពានទិន្នន័យឱ្យបានច្បាស់លាស់ ដែលផ្តល់អាទិភាពដល់ការការពារអ្នកប្រើប្រាស់ និងតម្លាភាព។
- ទី៤. សម្រាប់អ្នកប្រើប្រាស់ ឧប្បត្តិហេតុនេះបង្ហាញពីសារៈសំខាន់នៃការត្រួតពិនិត្យព័ត៌មានផ្ទាល់ខ្លួនឱ្យបានសកម្ម ហើយអ្នកគួរចាំបាច់ត្រូវប្រើប្រាស់ឧបករណ៍ ដូចជា សេវាកម្មត្រួតពិនិត្យឥណទាន ការជូនដំណឹងអំពីការក្លែងបន្លំ និងការការពារការលួចអត្តសញ្ញាណ ដើម្បីអាចជួយកាត់បន្ថយហានិភ័យនៃការបំពានទិន្នន័យ។

VI. សេចក្តីសន្និដ្ឋាន

ការវិវត្តយ៉ាងឆាប់រហ័សនៃបច្ចេកវិទ្យាបានធ្វើឱ្យមានការផ្លាស់ប្តូរយ៉ាងខ្លាំងលើការគ្រប់គ្រងទិន្នន័យរបស់បុគ្គល និងស្ថាប័ន ដែលទាមទារចាំបាច់ឱ្យមានវិធានសុវត្ថិភាពទិន្នន័យដ៏រឹងមាំ។ សុវត្ថិភាពទិន្នន័យគឺជាដំណើរការនៃការការពារព័ត៌មានឌីជីថលពីការលួច ឬការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត។ សុវត្ថិភាពទិន្នន័យរួមបញ្ចូលនូវការអនុវត្តបច្ចេកវិទ្យា និងគោលនយោបាយជាច្រើនដែលត្រូវបានរចនាឡើង ដើម្បីធានាឱ្យបាននូវ Confidentiality, Integrity, Authenticity និង Availability ហើយបានផ្តល់ឱ្យនូវអត្ថប្រយោជន៍ជាច្រើន ដូចជា ជួយការពារការបាត់បង់ ឬការបំពានលើទិន្នន័យសំខាន់ ឬរសើប, រក្សាទំនុកចិត្តរបស់អតិថិជន និងការពារកេរ្តិ៍ឈ្មោះរបស់ស្ថាប័ន, ផ្តល់ឱ្យនូវឧត្តមភាពប្រកួតប្រជែង និងជួយស្ថាប័ន និងអាជីវកម្មជៀសវាងការចំណាយបន្ថែម។ ដោយមើលឃើញពីសារៈសំខាន់នេះ រដ្ឋាភិបាលកម្ពុជាបានសម្រេចដាក់ចេញនូវការតាក់តែងសេចក្តីព្រៀងច្បាប់ និងអនុក្រឹតជាច្រើន ក៏ដូចជាសហការជាមួយភាគីពាក់ព័ន្ធនានា ដើម្បីលើកកម្ពស់វិធានការសុវត្ថិភាពទិន្នន័យឱ្យកាន់តែរឹងមាំនៅកម្ពុជា។ ដូច្នេះ ការដាក់ចេញនូវវិធានការសុវត្ថិភាពទិន្នន័យដ៏រឹងមាំនេះ ត្រូវបានចាត់ទុកថាពិតជាមានសារៈសំខាន់ ដែលចាំបាច់ត្រូវមានការយកចិត្ត

ទុកដាក់បន្ថែមទៀតពីគ្រប់ភាគីពាក់ព័ន្ធក្នុងការជួយជំរុញការងារនេះ ដើម្បីជៀសវាងការខាតបង់ដូចករណីការបំពានទិន្នន័យ Equifax។

ឯកសារយោង

- *Data Security vs Data Privacy vs Data Protection: Understanding the Key Differences*, ចេញផ្សាយថ្ងៃទី១៣ ខែមីនា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី៩ ខែមករា ឆ្នាំ២០២៥, *https://www.sisainfosec.com/blogs/data-security-vs-data-privacy-vs-data-protection-understanding-the-key-differences/#:~:text=Can%20you%20have%20data%20privacy,from%20unauthorized%20access%20or%20breaches.*
- *Data Security Meaning And Definition*, ចូលអានថ្ងៃទី៥ ខែមករា ឆ្នាំ២០២៥, *https://www.fortinet.com/resources/cyberglossary/data-security*
- *What is Data Security?*, ចូលអានថ្ងៃទី៦ ខែមករា ឆ្នាំ២០២៥, *https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-security/*
- *Data Privacy vs. Data Security: Definitions and Differences*, ចេញផ្សាយថ្ងៃទី៦ ខែធ្នូ ឆ្នាំ២០២៣, ចូលអានថ្ងៃទី៩ ខែមករា ឆ្នាំ២០២៥, *https://atlan.com/data-privacy-vs-data-security/#:~:text=To%20achieve%20robust%20data%20privacy,be%20extremely%20challenging%20and%20risky.*
- *Data in Transit*, ចូលអានថ្ងៃទី៩ ខែមករា ឆ្នាំ២០២៥, *https://www.imperva.com/learn/data-security/data-in-transit/*
- *What Is Internet Security?*, ចូលអានថ្ងៃទី៩ ខែមករា ឆ្នាំ២០២៥, *https://www.trellix.com/security-awareness/cybersecurity/what-is-internet-security/*
- *The Impact of AI and Machine Learning in Data Security: Elevating Protection for the Digital Age*, ចេញផ្សាយថ្ងៃទី២៨ ខែមីនា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២០ ខែមករា ឆ្នាំ២០២៥, *https://www.linkedin.com/pulse/impact-ai-machine-learning-data-security-elevating-protection-obgof*
- *The Role of AI and Machine Learning in Data Security*, ចូលអានថ្ងៃទី២០ ខែមករា ឆ្នាំ២០២៥, *https://accushred.net/blog/the-role-of-ai-and-machine-learning-in-data-security/*
- *Equifax Data Breach Settlement*, ចេញផ្សាយខែវិច្ឆិកា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៨ ខែមករា ឆ្នាំ២០២៥, *https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement*
- *Data security: trends and technologies for 2024*, ចេញផ្សាយថ្ងៃទី១៦ ខែកក្កដា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://www.lumiun.com/blog/en/data-security-trends-and-technologies-for-2024/*
- *What is SOAR (security orchestration, automation and response)?*, ចេញផ្សាយថ្ងៃទី៨ ខែកុម្ភៈ ឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://www.ibm.com/think/topics/security-orchestration-automation-response*
- *Better Protect your Data with Multi-Factor Authentication*, ចេញផ្សាយខែកញ្ញា ឆ្នាំ២០២២, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://sensortower.com/blog/better-protect-your-data-with-multi-factor-authentication*
- *4 Components of Data Security*, ចូលអានថ្ងៃទី២៨ ខែមករា ឆ្នាំ២០២៥, *https://www.aptimized.com/blogs/news/4-components-of-data-security*

- *3 Main Components of Data Security*, ចេញផ្សាយថ្ងៃទី១៣ ខែវិច្ឆិកា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២០ ខែមករា ឆ្នាំ២០២៥, *https://knowledgewebcasts.com/3-main-components-of-data-security/*
- *What is Multi-Factor Authentication (MFA)?*, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://cybersecurity.asee.io/authentication-and-identity/*
- *What is cloud data security? Benefits and solutions*, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://cloud.google.com/learn/what-is-cloud-data-security#what-are-the-benefits-of-cloud-data-security*
- *Data Security Importance: Definition, Types, and More*, ចេញផ្សាយថ្ងៃទី៨ ខែតុលា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://www.designrush.com/agency/cybersecurity/trends/why-is-data-security-important*
- *Benefits Of Data Security: Protect Your Data And Advance Your Business*, ចេញផ្សាយថ្ងៃទី២៦ ខែមករា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://elnion.com/2023/12/27/benefits-of-data-security-part-1-protect-your-data-and-advance-your-business/*
- ក្រុមហ៊ុនវីសា ប្រកាសពីផែនការពង្រឹងសុវត្ថិភាពលើការទូទាត់ប្រាក់ដើម្បីគាំទ្រក្នុងការទូទាត់ ដោយមិនប្រើសាច់ប្រាក់សុទ្ធនៅក្នុងប្រទេសកម្ពុជា, ចេញផ្សាយថ្ងៃទី៤ ខែកញ្ញា ឆ្នាំ២០១៩, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥, *https://www.information.gov.kh/articles/22039*
- អនុក្រឹត ស្តីពី ការគ្រប់គ្រង ការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គល, ចេញផ្សាយថ្ងៃទី២២ ខែធ្នូ ឆ្នាំ២០២១, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥
- អត្ថបទសិក្សា ស្តីពី "សន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិតក្នុងបរិបទកម្ពុជា", ចេញផ្សាយថ្ងៃទី៣១ ខែមករា ឆ្នាំ២០២២, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥
- អនុក្រឹត្យ ស្តីពី ការរៀបចំនិងការប្រព្រឹត្តទៅរបស់គណៈកម្មាធិការសន្តិសុខឌីជីថល, ចេញផ្សាយថ្ងៃទី៧ ខែមីនា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥
- គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥, ចេញផ្សាយខែមករា ឆ្នាំ២០២២, ចូលអានថ្ងៃទី២៤ ខែមករា ឆ្នាំ២០២៥
- *Equifax data breach FAQ: What happened, who was affected, what was the impact?*, ចេញផ្សាយថ្ងៃទី១២ ខែកុម្ភៈ ឆ្នាំ២០២០, ចូលអានថ្ងៃទី២៨ ខែមករា ឆ្នាំ២០២៥, *https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html*
- *Average cost of a data breach worldwide from 2014 to 2024*, ចេញថ្ងៃទី១១ ខែកញ្ញា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៩ ខែមករា ឆ្នាំ២០២៥, *https://www.statista.com/statistics/987474/global-average-cost-data-breach/*

កម្ពុជា ៤.0 - Cambodia 4.0

កម្ពុជា ៤.0 Cambodia 4.0

កម្ពុជា ៤.0 - Cambodia 4.0

កម្ពុជា ៤.0 - Cambodia 4.0

www.cambodia4point0.org

cambodia_4.0

កម្ពុជា ៤.0 - Cambodia 4.0

Cambodia 4.0 Center

គាំទ្រដោយ