ОЦІНКА РИЗИКІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ КРИТИЧНИХ РЕСУРСІВ

Заболотний В.В., Корнієнко Б.Я., Галата Л.П.

Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ, Україна

Незалежно від кроків, зроблених для захисту АСУ ТП, завжди можливо, що це може бути скомпрометовано навмисним або ненавмисним інцидентом. Наступні симптоми можуть виникати внаслідок нормальних мережевих проблем, але коли з'являються кілька симптомів, шаблон може вказувати на те, що система знаходиться під атакою і може бути варто дослідити далі. Якщо супротивник є кваліфікованим, то не зовсім очевидним є те, що атака триває.

Симптомами інциденту може будь-яка вказана нижче ситуація:

- незвичайно високий мережевий трафік;
- закінчення місця на диску або його значне зменшення;
- незвичайно велике використання центрального процесора;
- створення нових облікових записів користувачів;
- спроба або використання облікових записів рівня адміністратора;
- блокування облікових записів;
- використання облікового запису працівника, коли він не на роботі;
- очищення журналу системи;
- попередження антивірусного програмного забезпечення;
- вимкнене антивірусне програмне забезпечення;
- під’єднання до зовнішніх IP-адрес;
- запити про інформацію про систему (спроби соціальної інженерії);
- неочікувані зміни у конфігурації;
- неочікуване вимкнення системи.

Щоб мінімізувати наслідки цих вторгнень, необхідно спланувати відповідь. Планування реагування на інциденти визначає процедури, яких слід дотримуватися, коли відбувається вторгнення. Посібник з керування інцидентами з комп'ютерною безпекою, надає вказівки щодо планування реагування на інциденти, які можуть містити такі елементи:

– класифікація інцидентів. Різні типи інцидентів АСУ ТП повинні бути ідентифіковані та класифіковані як потенційні наслідки, щоб можна було сформулювати відповідну реакцію для кожного потенційного інциденту;

– відповіді на загрози. Є кілька відповідей, які можуть бути прийняті у випадку інциденту. Вони варіюються від бездіяльності до повного виключення системи (хоча повне вимкнення АСУ ТП є дуже малоймовірним). Відповідь буде залежати від типу інциденту та його впливу на АСУ ТП і контрольований фізичний процес. Необхідно підготувати письмовий план, що документує типи інцидентів та відповіді на кожен тип. Це дасть вказівки в часи, коли може виникнути плутанина або напруга через інцидент. Цей план повинен включати покрокові дії, які повинні виконувати різні організації. Якщо існують вимоги щодо звітності, їх слід зауважити, а також, де слід скласти звіт, та телефонні номери, щоб зменшити плутанину звітності;

– дії з відновлення працездатності. Результати вторгнення можуть бути незначними, або вторгнення може спричинити багато проблем у АСУ ТП. Необхідно провести аналіз ризиків для визначення чутливості фізичної системи, яка контролюється, до режимів відмови в системі. У кожному випадку покрокові дії з відновлення повинні бути задокументовані таким чином, щоб система могла бути повернута до нормальних операцій якомога швидше і безпечніше. Дії відновлення для втручання, які впливають на роботу АСУ ТП, будуть тісно узгоджені з планом відновлення після аварії в системі, і повинні враховувати вже створене планування та координацію;

Під час підготовки плану реагування на інциденти необхідно отримати інформацію від різних зацікавлених сторін, включаючи операції, інжиніринг, інформаційні технології, постачальники системної підтримки, управління, організовану працю, правову та безпечну діяльність. Ці зацікавлені сторони також повинні переглянути та затвердити план.

Необхідно запровадити офіційну програму управління змінами та застосувати процедури для того, щоб всі зміни в мережі системи відповідали тим самим вимогам безпеки, що й оригінальні компоненти, визначені в оцінці активів та пов'язані з ними плани оцінки ризиків і пом'якшення. Оцінка ризику повинна проводитися на всіх змінах мережі, які можуть вплинути на безпеку, включаючи зміни в конфігурації, додавання мережевих компонентів та встановлення

програмного забезпечення. Також можуть знадобитися зміни в політиці та процедурах. Поточна конфігурація мережі АСУ ТП і конфігурації пристроїв повинні завжди бути відомими і задокументовані.

Плани на випадок надзвичайних ситуацій повинні охоплювати весь спектр невдач або проблем, які можуть бути спричинені кіберінцидентами. Плани на випадок надзвичайних ситуацій повинні включати процедури відновлення систем від відомих дійсних резервних копій, відокремлення систем від усіх несуттєвих перешкод і з'єднань, які могли б дозволити вторгнення в кібербезпеку, і альтернативи для досягнення необхідних інтерфейсів і координації. Співробітники повинні бути навчені і знайомі з змістом планів на випадок надзвичайних ситуацій. Плани дій на випадок надзвичайних ситуацій повинні періодично переглядатися з працівниками, відповідальними за відновлення АСУ ТП, і перевірятися, щоб гарантувати, що вони продовжують виконувати свої цілі. Організації також мають плани безперервності бізнесу та плани відновлення після аварії, які тісно пов'язані з планами на випадок надзвичайних ситуацій.

Планування безперервності бізнесу вирішує загальну проблему збереження або відновлення виробництва у випадку переривання. Ці перерви можуть приймати форму стихійного лиха (наприклад, урагану, торнадо, землетрусу, повені), ненавмисної техногенної події (наприклад, випадкове пошкодження обладнання, пожежа або вибух, помилка оператора), умисне техногенне подія (наприклад, атака бомбою, вогнепальною зброєю або вандалізмом, зловмисником або вірусом) або збоєм обладнання. З точки зору потенційного відключення, це може включати типові часові проміжки днів, тижнів або місяців для відновлення після стихійного лиха або хвилини або години для відновлення після зараження шкідливим програмним забезпеченням або механічної чи електричної несправності. Оскільки часто існує окрема дисципліна, що стосується надійності та електромеханічного обслуговування, деякі організації вибирають визначення безперервності бізнесу таким чином, що виключає ці джерела відмови. Оскільки безперервність бізнесу також стосується головним чином довгострокових наслідків відключень виробництва, деякі організації також вирішили розмістити обмеження на мінімальне переривання на ризики, які необхідно розглянути. Для цілей кібербезпеки АСУ ТП рекомендується не застосовувати жодного з цих обмежень. Довготривалі відключення (аварійне відновлення) та короткострокові відключення (оперативне відновлення) повинні бути розглянуті. Оскільки деякі з

цих потенційних перерв пов'язані з техногенними подіями, важливо також співпрацювати з організацією фізичної безпеки, щоб зрозуміти відносні ризики цих подій та фізичні заходи безпеки, які існують для запобігання їх. Також важливо, щоб організація фізичної безпеки зрозуміла, в яких областях системи придбання та управління даними на виробничому майданчику міститься ризик більш високого рівня.

Після визначення цілей відновлення слід створити перелік потенційних перерв і розробити та описати процедуру відновлення. Для більшості перерв у менших масштабах ремонту та заміни діяльності на основі критичних запасів запасних частин буде достатньо для досягнення цілей відновлення. Коли це не відповідає дійсності, необхідно розробити резервні плани. У зв'язку з потенційними витратами та важливістю цих планів на випадок надзвичайних ситуацій, вони повинні бути переглянуті разом з керівниками, відповідальними за планування безперервності бізнесу, щоб переконатися, що вони є виправданими. Після того, як процедури відновлення будуть задокументовані, слід розробити графік для перевірки частини або всіх процедур відновлення. Особлива увага повинна приділятися перевірці резервних копій даних конфігурації системи та даних про продукт або продукцію. Приклади даних конфігурації системи включають в себе резервні копії конфігурації комп'ютера, резервні копії конфігурації програми, ліміти операційного контролю, контрольні смуги та задані значення для операцій попереднього інциденту для всіх програмних пристроїв АСУ ТП. Вони не тільки повинні бути перевірені, коли вони виробляються, але й процедури, які слідують за їх зберігання, також повинні періодично переглядатися, щоб переконатися, що резервні копії зберігаються в умовах навколишнього середовища, які не зроблять їх непридатними і що вони зберігаються в безпечному місці, тому вони можуть бути швидко отримані уповноваженими особами, коли це необхідно.

Література

1. Корнієнко Б.Я. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. Моделювання та інформаційні технології. 2018. Вип. 83. С. 34-41.

2. Корнієнко Б.Я. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. Наукоємні технології. 2017. № 4 (36). С. 316 - 322.

3. Корнієнко Б.Я., Максімов Ю.О., Марутовська Н.М. Прикладні програми управління інформаційними ризиками. Захист інформації. 2012. № 4 (57). С. 60 – 64. DOI: 10.18372/2410-7840.14.3493 (ukr).

4. Корнієнко Б.Я., Галата Л.П. Оптимізація системи захисту інформації корпоративної мережі. Математичне та комп'ютерне моделювання. Серія: Технічні науки, Випуск 19, 2019. - С. 56-62.

5. Korniyenko B., Galata L. Implementation of the information resources protection based on the CentOS operating system. Conference Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON -2019) July 2 – 6, 2019, Lviv, Ukraine. - pp. 1007-1011.

6. Галата Л.П., Корнієнко Б.Я., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. Наукоємні технології, Том 43, № 3, 2019. – С. 300 – 306.

7. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. Conference Proceedings of 2019 IEEE Inernational Conference on Advanced Trends in Information Theory (IEEE ATIT -2019) Dezember 18 – 20, 2019, Kyiv, Ukraine. - pp. 244-248.

8. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019) Kyiv, Ukraine, November 28, 2019. Vol-2577. P.281-291.

9. Корниенко Б.Я. Кибернетическая безопасность – операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2017. – 122 с.

10. Korniyenko B.Y., Galata L.P. Design and research of mathematical model for information security system in computer network. Наукоємні технології. – 2017, № 2 (34), С. 114 - 118.

11. Корниенко Б.Я. Информационная безопасность и технологии компьютерных сетей : монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с.

12. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. Sciences of Europe. – 2016. – V. 2. – No 2 (2). – P. 61 -63.

13. Korniyenko B. The classification of information technologies and control systems. International scientific journal. – 2016. –№ 2. – P. 78 - 81.

14. Корнієнко Б.Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив :монографія. – К.: Вид-во Аграр Медіа Груп, 2014. – 288 с.

15. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources / B. Korniyenko, //CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) Kyiv, Ukraine, November 27, 2018, Vol-2318, - P. 176-187, urn:nbn:de:0074-2318-4

16. Korniyenko B.Y., Borzenkova S.V., Ladieva L.R. Research of three-phase mathematical model of dehydration and granulation process in the fluidized bed / B.Y. Korniyenko, S.V. Borzenkova, L.R. Ladieva // ARPN Journal of Engineering and Applied Sciences Volume 14, Issue 12, June 2019, Pages 2329-2332.

17. Zhulynskyi A.A., Ladieva L.R., Korniyenko B.Y. Parametric identification of the process of contact membrane distillation/ A.A. Zhulynskyi, L.R. Ladieva, B.Y. Korniyenko // ARPN Journal of Engineering and Applied Sciences Volume 14, Issue 17, September 2019, Pages 3108-3112.

18. Korniyenko B., Ladieva L. Mathematical Modeling Dynamics of the Process Dehydration and Granulation in the Fluidized Bed. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing, vol 1247. Springer, Cham, pp. 18-30. https://doi.org/10.1007/978-3-030-55506-1_2

19. Korniyenko, B., Ladieva, L., Galata, L. Control system for the production of mineral fertilizers in a granulator with a fluidized bed. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, pp. 307–310.

20. Ladieva, L., Kozanevych, Z., Klusta, T., Korniyenko, B. System of control of the process of alkylation of benzene with peripene in the liquid phase. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, pp. 311–314.