КОНТРОЛЬ ДОСТУПУ ДО АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВИРОБНИЦТВОМ МІНЕРАЛЬНИХ ДОБРИВ

Заболотний В.В., Корнієнко Б.Я.

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

Аутентифікація описує процес позитивної ідентифікації потенційних користувачів мережі, хостів, програм, служб і ресурсів, використовуючи комбінацію факторів ідентифікації або облікових даних. Результат цього процесу аутентифікації потім стає основою для дозволу або відмови від подальших дій (наприклад, коли банкомат запитує PIN-код). На основі визначення автентичності система може або не може дозволити потенційному користувачеві отримати доступ до своїх ресурсів. Авторизація - це процес визначення того, кому і що має бути дозволено мати доступ до певного ресурсу; контроль доступу - це механізм забезпечення авторизації.

Існує кілька можливих факторів для визначення автентичності особи, пристрою або системи, включаючи те, що ви знаєте, те, що у вас є або те, ким ви є. Наприклад, аутентифікація може бути заснована на чомусь, що ви знаєте (наприклад, PIN-код або пароль), чомусь, що ви маєте (наприклад, ключ, ключ, смарт-карта), тому, ким ви є як біологічна характеристика (наприклад, відбиток пальця, підпис сітківки), розташуванні (наприклад, доступ до системи глобального позиціонування). Загалом, чим більше факторів, які використовуються в процесі аутентифікації, тим надійнішим буде процес. При використанні двох або більше факторів процес відомий як багатофакторна аутентифікація.

Комп'ютерні системи в середовищі АСУ ТП зазвичай використовують традиційні паролі для автентифікації. Постачальники систем управління часто постачають системи з паролями за замовчуванням. Ці паролі встановлені на заводі і часто легко вгадуються або рідко змінюються, що створює додаткові ризики для безпеки.

Якщо противник отримує доступ до носіїв резервної копії, пов'язаних з АСУ ТП, він може надати цінні дані для запуску атаки. Відновлення файлу аутентифікації з резервних копій може дозволити противнику запускати засоби

для злому паролів і витягувати корисні паролі. Крім того, резервні копії зазвичай містять імена машин, IP-адреси, номери версій програмного забезпечення, імена користувачів та інші дані, корисні при плануванні атаки.

Використання будь-яких несанкціонованих компакт-дисків, DVD-дисків, дискети, USB-накопичувачів або подібних знімних носіїв на будь-якому вузлі, який є частиною або підключено до АСУ ТП, не допускається для запобігання впровадженню шкідливого програмного забезпечення або випадкової втрати або крадіжки даних.

Фізичний захист кібер-компонентів і даних, пов'язаних з АСУ ТП, має розглядатися як частина загальної безпеки заводу. Безпека в багатьох об'єктах системи тісно пов'язана з безпекою підприємства. Основна мета полягає в тому, щоб уникнути небезпечних ситуацій, не заважаючи їм виконувати свою роботу або виконувати надзвичайні процедури. Фізичні засоби безпеки - це будь-які фізичні заходи, активні або пасивні, які обмежують фізичний доступ до будь-яких інформаційних ресурсів в середовищі АСУ ТП. Ці заходи застосовуються для запобігання багатьох видів небажаних ефектів, включаючи:

– фізичний доступ зловмисників до чутливих місць;

– фізична модифікація, маніпулювання, крадіжка або інше видалення або знищення існуючих систем, інфраструктури, комунікаційних інтерфейсів, персоналу або фізичних місць;

– несанкціоноване спостереження за чутливими інформаційними ресурсами через візуальне спостереження, записки, фотографії або інші засоби;

– запобігання несанкціонованому впровадженню нових систем, інфраструктури, комунікаційних інтерфейсів або іншого обладнання;

– запобігання несанкціонованому впровадженню пристроїв, навмисно створених для того, щоб викликати апаратні маніпуляції, підслуховування комунікацій або інші шкідливі наслідки.

Отримання фізичного доступу до контрольної кімнати або компонентів системи управління часто передбачає отримання логічного доступу до системи управління технологічними процесами. Крім того, наявність логічного доступу до систем, таких як основні сервери та комп'ютери контрольної кімнати, дозволяє противнику здійснювати контроль над фізичним процесом.

Поглиблене рішення захисту фізичної безпеки має містити такі атрибути:

– захист фізичних локацій. Створення декількох фізичних бар'єрів, як активних, так і пасивних, навколо будівель, споруд, приміщень, обладнання або інших інформаційних ресурсів, встановлює ці фізичні периметри безпеки.;

– контроль доступу. Системи контролю доступу повинні забезпечити доступ тільки до уповноважених осіб до контрольованих просторів. Система контролю доступу повинна бути гнучкою. Потреба в доступі може базуватися на часі (денна або нічна зміна), рівні підготовки, статусу зайнятості, призначення на роботу, статусі і безлічі інших факторів.;

– система слідкування за доступом. Системи контролю доступу включають камери і відеокамери, датчики та різні типи систем ідентифікації. Прикладами таких систем є камери, які контролюють стоянки чи магазини.;

– системи обмеження доступу. Системи обмеження доступу можуть використовувати комбінацію пристроїв для фізичного контролю або запобігання доступу до захищених ресурсів. Системи обмеження доступу включають як активні, так і пасивні пристрої безпеки, такі як огорожі, двері, сейфи, ворота та охоронні пристрої. Вони часто поєднуються з системами ідентифікації та моніторингу для забезпечення рольового доступу для конкретних осіб або груп осіб.

– відслідковування людей та активів. Розміщення людей та транспортних засобів у великих об'єктах є дуже важливим з міркувань безпеки. Технології розміщення активів можуть бути використані для відстеження переміщень людей і транспортних засобів на заводі, для забезпечення їх перебування в дозволених зонах, для визначення персоналу, який потребує допомоги, і для підтримки реагування на надзвичайні ситуації;

– фактори навколишнього середовища. При вирішенні проблем безпеки системи та даних важливо враховувати фактори навколишнього середовища. Наприклад, якщо підприємство знаходиться у запиленому середовищі, системи повинні бути розміщені у фільтрованому середовищі. Це особливо важливо, якщо пил, ймовірно, є провідним або магнітним, як у випадку з вузлами, які обробляють вугілля або залізо. Якщо присутня вібрація, системи повинні бути встановлені на гумових втулках, щоб запобігти виникненню проблем з дисками та з'єднанням. Крім того, середовища, що містять системи та носії (наприклад, резервні стрічки, дискети), повинні мати стабільну температуру та вологість.

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.