DOI 10.15276/imms.v11.no4.358
УДК 004.716:621.391

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 4, pp. 358-364

ЗАХИСТ КОРПОРАТИВНИХ МЕРЕЖ ВІД ЛЮДСЬКОГО ВПЛИВУ ЗА ДОПОМОГОЮ ТЕХНІЧНИХ ЗАСОБІВ

Ю.М. Ткач[1], О.О. Яковлєв[2], Т.А. Лисиця[2]

[1]Національний університет «Чернігівська політехніка»
Чернігів, вул.Шевченка, 95. E-mail: tkachym79@gmail.com
[2]АТ «Альфа-банк». м. Чернігів, просп. Перемоги, 62. E-mail: samehada@i.ua

Широке використання комп'ютерних технологій в автоматизованих системах обробки даних та управлінні загострило проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має ряд специфічних особливостей, пов'язаних з тим, що інформація, яка не є строго пов'язаною з носієм, може бути легко і швидко скопійована і передана по каналах зв'язку. У комп'ютерних мережах орієнтована інформація належить певним людям, які перебувають в особистій ініціативі або відповідно до офіційних обов'язків, і лише вони мають право використовувати цю інформацію. Така інформація повинна бути захищена від усіх форм зовнішнього втручання, особливо від читання та копіювання цієї інформації, людьми, які не мають права доступу до цієї інформації. Метою роботи є дослідження методів захисту корпоративної мережі, збір та аналіз інформації з приводу політик безпеки. Тому було проведено опитування серед експертів, для виявлення найважливіших місць у технічному захисті, що можуть бути використані проти методів соціальної інженерії. Для цього результати опитування було проаналізовано та вибрано основні критерії. Далі, використовуючи матриці переваг та математичний аналіз було виявлено які критерії з обраних є найважливішими, та вказано фактори котрі можуть як позитивно так і негативно вплинути на обрані основні критерії. Це необхідно для того, щоб розуміти як саме можна захиститися від методів соціальної інженерії.

Ключові слова: інформаційна безпека; людський фактор; політика безпеки; автентифікація; ідентифікація; контроль доступу.

Вступ

На даний час основною проблемою в захисті інформації є людський фактор, а не технічний. Найбільш вразливою ланкою інформаційних систем є саме людина, на котру дуже легко вплинути. Саме тому, дуже важливо створити політику безпеки. Структура, в якій організація прагне задовольнити свої потреби в інформаційній безпеці, кодифікується як політика безпеки. Політика безпеки - це стисла заява відповідальних за систему (наприклад, вищого керівництва) інформаційних цінностей, відповідальності за захист та організаційних зобов'язань.

Ми знаємо дуже велику кількість загроз інформації, яка може бути реалізована як сторонніми зловмисниками, так і сторонніми особами.

Проблеми, що виникають при передачі інформації про безпеку, коли комп'ютерні мережі можна розділити на три основні типи:

– перехоплення - цілісність інформації, що зберігається, але її конфіденційність порушена;

– інформація при заміщення авторства - ця проблема може мати серйозні наслідки. Наприклад, якщо хтось може надіслати лист від вашого імені (такий тип шахрайства називається підробкою) або веб-сервер може робити вигляд, що зберігає в електронному вигляді, приймати замовлення, номери кредитних карток, але не надсилати ніяких товарів.

– модифікація інформації - в цьому випадку оригінальне повідомлення редагується або змінюється повністю, а інше надсилається одержувачу.

Важливості питань інформаційної безпеки приділяють увагу численні науковці, у тому числі й іноземні. Аналіз останніх досліджень і публікацій свідчить про те, що певні аспекти проблем інформаційної безпеки досліджують у наукових працях Н. Стоянов, В. Литвинов, И. Шкиттер, Х. Трунова, Todd Rosenberry, Shiju Sathyadevan, Venkat Rangan, Krishnashree Achuthan, а також досліджують в різних інститутах National Research Council.

Мета і задачі дослідження

Дослідження методів захисту корпоративної мережі, збір та аналіз інформації з приводу політики безпеки. Розгляд та аналіз поняття інфомаційної безпеки та ознайомитись з основними принципами запобігання порушень безпеки. Розгляд та аналіз поняття політики безпеки та провести опитування з приводу найважливіших місць захисту від соціальної інженерії. Розгляд та аналіз на рівні корпоративних мереж та методи їх захисту від втручать ззовні та зсередини

Основна частина

Організації та люди, які використовують комп’ютери, можуть описати свої потреби в інформаційній безпеці та довірі до систем з точки зору трьох основних вимог:

1. Конфіденційність: контроль, хто отримує можливість читати інформацію;
2. Цілісність: гарантування того, що інформація та програми змінюються лише у визначеному та дозволеному порядку; і
3. Доступність: гарантування постійного доступу авторизованих користувачів до інформації та ресурсів [1].

Ці три вимоги можуть підкреслюватися по-різному в різних додатках. Для національної системи оборони головним завданням може бути забезпечення конфіденційності секретної інформації, тоді як система переказу коштів може вимагати суворого контролю цілісності. Вимоги до програм, які підключені до зовнішніх систем, будуть відрізнятися від вимог до програм без такого взаємозв'язку. Таким чином, конкретні вимоги та засоби управління інформаційною безпекою можуть відрізнятися.

Структура, в якій організація прагне задовольнити свої потреби в інформаційній безпеці, кодифікується як політика безпеки. Політика безпеки - це стисла заява відповідальних за систему (наприклад, вищого керівництва) інформаційних цінностей, відповідальності за захист та організаційних зобов'язань [2]. Можна реалізувати таку політику, вживаючи конкретні дії, керуючись принципами управлінського контролю та використовуючи конкретні стандарти, процедури та механізми безпеки. І навпаки, вибір стандартів, процедур та механізмів повинен керуватися політикою, щоб вона була найбільш ефективною.

Для того, щоб бути корисним, політика безпеки повинна не лише визначати потребу в безпеці (наприклад, у конфіденційності - дані повинні розголошуватися лише уповноваженим особам), але також враховувати коло обставин, за яких ця потреба повинна бути виконана, та відповідні операційні стандарти . Без цієї другої частини політика безпеки є настільки загальною, що виявляється марною (хоча друга частина може бути реалізована за допомогою процедур та стандартів, встановлених для реалізації політики). У будь-яких конкретних обставинах деякі загрози є більш вірогідними, ніж інші, і розсудливий розробник політики повинен оцінити загрози, визначити рівень занепокоєння кожному та визначити політику, щодо якої загрозам слід протистояти.

Запобігання порушенням безпеки - основні принципи

Елементи управління призначені для спрямування операцій у правильних напрямках, запобігання або виявлення зловживань та шкідливих помилок, а також раннього попередження про вразливі місця. Організації майже в усіх напрямках діяльності встановили контроль на основі таких ключових принципів:

– Індивідуальна підзвітність,
– Аудит,
– Поділ обов'язку[3].

Ці принципи, визнані в тій чи іншій формі століттями, є основою операційних процедур до комп'ютерів, які дуже добре зрозумілі.

Індивідуальна підзвітність відповідає на питання: Хто відповідає за цю заяву чи дію? Його мета - відстежувати те, що сталося, хто мав доступ до інформації та ресурсів та які дії були вжиті. У будь-якій реальній системі є багато причин, чому фактична експлуатація не завжди може відображати початкові наміри власників: люди роблять помилки, система має помилки, система вразлива до певних атак, широка політика не була правильно перекладена в детальних специфікаціях, господарі передумали тощо.

Для підтримки принципу індивідуальної підзвітності потрібна послуга, яка називається автентифікацією користувачів. Без надійної ідентифікації не може бути відповідальності. Таким чином, автентифікація є вирішальним підґрунтям інформаційної безпеки. Багато систем було проникнуто, коли слабкі або погано керовані служби автентифікації були скомпрометовані, наприклад, вгадуючи неправильно вибрані паролі.

В ідеалі всебічний спектр заходів безпеки забезпечить належну підтримку конфіденційності, цілісності та доступності комп’ютерних систем. На практиці неможливо дати залізні гарантії. Єдиний рецепт ідеальної безпеки - це ідеальна ізоляція: нічого, нічого назовні. Це недоцільно, і тому політика безпеки завжди відображатиме компроміси між вартістю та ризиком. Активи, що підлягають захисту, слід класифікувати за вартістю, вразливі місця за важливістю, а ризики - за ступенем серйозності, а також відповідно встановити захисні заходи. Слід визнати залишкові вразливості[4].

Планування програми безпеки приблизно нагадує купівлю страховки. Організація враховує наступне:

– Вартість активів, що захищаються.

– Вразливості системи: можливі типи компромісів, як користувачів, так і систем. Яку шкоду може нанести людина, що стоїть перед автоматизованою касовою машиною? А як щодо людини, яка стоїть за цим?

– Загрози: чи існують супротивники для використання цих уразливостей? Чи є у них мотив, тобто щось здобути? Наскільки ймовірна атака в кожному випадку?

– Ризики: витрати на відмови та відновлення. Який найгірший достовірний вид невдачі? Можливості - це смерть, травми, компрометація національної безпеки, промисловий шпигунство, втрата особистого життя, фінансове шахрайство, фальсифікація виборів.

– Ступінь несхильності організації до ризику.

Звідси випливає приблизне уявлення про очікувані збитки. З іншого боку це:

– Доступні контрзаходи (засоби контролю та служби безпеки),
– Їх ефективність,
– Їх прямі витрати та альтернативні витрати на їх встановлення.

Потім плани безпеки стають діловим рішенням, можливо, пом'якшеним юридичними вимогами та врахуванням зовнішніх.

В ідеалі контроль вибирається в результаті ретельного аналізу. На практиці найважливішим фактором є те, які засоби контролю доступні. Більшість покупців комп'ютерних систем не можуть дозволити собі мати систему, розроблену з нуля для

задоволення своїх потреб, обставина, яка здається особливо вірною у випадку потреб безпеки. Таким чином, замовник зводиться до вибору з числа вже існуючих рішень з надією, що одне з них відповідатиме визначеним потребам.

Оскільки безпека - явище слабкої ланки, програма захисту повинна бути багатовимірною. Незалежно від цілей політики безпеки, не можна повністю ігнорувати будь-яку з трьох основних вимог - конфіденційність, цілісність та доступність - які підтримують одна одну. Наприклад, конфіденційність необхідна для захисту паролів. Паролі, у свою чергу, сприяють цілісності системи, контролюючи доступ та забезпечуючи основу для індивідуальної відповідальності[5]. Самі особи, що контролюють конфіденційність, повинні бути несприйнятливі до фальсифікацій - це питання доброчесності. І в тому випадку, якщо щось піде не так, адміністративний персонал і персонал, що займається технічним обслуговуванням, повинен мати можливість втрутитися, щоб виправити ситуацію - проблема щодо наявності.

Ідентифікація користувача

Усі опитані вважали, що унікальна ідентифікація (ID) для кожного користувача та автоматичне призупинення посвідчення особи для певної кількості спроб несанкціонованого доступу є важливими. Здатність запобігти одночасному використанню посвідчення особи вважалася важливою для 90 відсотків опитаних осіб. Коментар полягав у тому, що цією можливістю слід керувати на основі ідентифікатора або джерела доступу.

Вісімдесят три відсотки опитаних погодились, що важливо, щоб дата, час та місце останнього використання були відображені користувачеві під час входу в систему. Зауважили, що ця функція також повинна бути доступна в інший час. Той самий номер вимагав можливості присвоєння користувачеві терміну дії для авторизації доступу до системи. Коментарі щодо цього пункту полягали в тому, що потрібна можливість вказати дату активного в майбутньому для ідентифікаторів і що потрібна можливість повідомити системного адміністратора про те, що термін дії ідентифікатора закінчується. Сімдесят три відсотки вважали, що можливість обмеження доступу до системи певним часом, днями, датами та / або з певних місць є надзвичайно важливою.

Перевірка або автентифікація користувача

Усі опитані вважали, що запобігання повторному використанню прострочених паролів, примусове змінення пароля в системі, постійне запрошення пароля та перевірка ідентифікатора та пароля під час входу - це всі необхідні заходи безпеки.

Дев'яносто сім відсотків вважали важливими можливості реалізації пароля із шести або більше буквено-цифрових символів та збереження паролів, зашифрованих у системі. Вісімдесят сім відсотків вважали, що автоматична перевірка для усунення простих паролів має бути важливою особливістю, хоча одна особа вважала, що в цьому випадку важко буде знати, на що перевіряти.

Шістдесят відсотків бачили можливість взаємодії з динамічним маркером пароля важливою функцією. Однією з рекомендацій було дослідити використання піктограм, які будуть призначені користувачам як керівництво для вибору значущих (легко запам'ятовуються) паролів. Тридцять три відсотки вважали генератор випадкових паролів важливим; 7 відсотків не хотіли одного.

Контроль доступу до файлів

Усі опитані вважали надзвичайно важливим мати можливість обмежити доступ до файлів, програм та баз даних. Лише 60 відсотків вважають, що можливість обмеження доступу до визначеного часу або доби повинна бути важливою. Хоча всі співробітники інформаційної безпеки фінансових організацій вважали, що така

можливість має бути надзвичайно важливою, принаймні деякі представники всіх інших категорій підприємств вважали за краще, щоб така функція була необов'язковою.

Вісімдесят три відсотки погодились з тим, що можливість виявлення та захисту вірусів та можливість очищення файлу під час видалення є найважливішими характеристиками. Додатковим зауваженням було те, що від продавців потрібно вимагати сертифікацію продукту на відсутність вірусів або люків. Сімдесят три відсотки вважали можливість шифрування конфіденційних даних обов'язковою, але один респондент висловився проти цієї функції, оскільки це може ускладнити відновлення після аварії (тобто, можливо, не вдасться отримати доступ до таких даних в надзвичайних ситуаціях під час обробки на іншому сайті). Дев'яносто п'ять відсотків вважали важливим вимагати виконання виробничих програм із захищеної виробничої бібліотеки, а також, якщо використовується шифрування, знищити відкритий текст під час процесу шифрування.

Управління терміналом

Усі опитані погодились, що запобігання показу паролів на екранах або звітах має бути важливим. Дев'яносто п'ять відсотків висловилися за автоматичну можливість виходу / виходу з режиму очікування як обов'язкову функцію. Коментар полягав у тому, що цю функцію слід змінювати за ідентифікатором.

Ідентифікація терміналів була здатністю, яку 87 відсотків вважали важливою, але лише дві третини вважали, що клеммний замок повинен бути включений до основної категорії. Додатковим зауваженням було те, що маркерний порт (для динамічного інтерфейсу пароля) повинен бути особливістю терміналів.

Спочатку було використано метод експертних оцінок, за яким чотири експерта на основі асоціацій та неординарних рішень обрали найважливіші критерії. Далі, для більш комплексного аналізу поставленої проблеми, було використано метод інверсії, завдяки чому відбулася різка зміна напряму пошуку рішень та виявлення абсолютно нових рішень. Сформульовані критерії вибору представлені в табл.1.

Таблиця 1

Критерії вибору рішень

№	Критерії	Опис критеріїв
1	Контроль доступу до файлів	Заборона або дозвіл доступу до файлів на основі ідентифікатора
2	Управління терміналом	Запобігання показу паролів на екранах, а також автоматичне блокування екранів при бездіяльності
3	Ідентифікація користувача	Розпізнавання користувача в системі, за допомогою ідентифікатора
4	Автентифікація користувача	Встановлення належності користувачеві інформації пред'явленого ним ідентифікатора

Відносну важливість переваг було визначено експертами за шкалою Сааті. Для заповнення матриці переваг було попарно порівняно кожен показник з іншими і, за шкалою Сааті, визначено перевагу для кожної пари(табл. 2)

Таблиця 2

Загальна матриця переваг

Критерії		**1**	**2**	**3**	**4**
Контроль доступу до файлів	**1**	1	0,5	2	3
Управління терміналом	**2**	2	1	2	3
Ідентифікація користувача	**3**	0,5	0,5	1	3
Автентифікація користувача	**4**	0,333	0,333	0,333	1
	Сума	2,2	4,8	6,3	9,0

Розрахуємо вектори локальних переваг (табл. 3-4)

Таблиця 3

Матриція нижчого рівня

Критерії		1	**2**	**3**	**4**
Контроль доступу до файлів	**1**	1	3	2	4
Управління терміналом	**2**	0,3	1	1	2
Ідентифікація користувача	**3**	0,5	1	1	2
Автентифікація користувача	**4**	0,25	0,5	0,5	1
	Сума	2,05	5,5	4,5	9

Таблиця 4

Матриця векторів локальних переваг

i / j	Головний власний вектор V_i	Вектор пріоритетів P_i	Сума по колонках S_j	Власне значення λmax $P_i S_j$
1	1,817121	0,45428	6	2,725681
2	0,669433	0,167358	2,3	0,384924
3	0,793701	0,198425	2,5	0,496063
4	0,39685	0,099213	1,25	0,124016
Сума	3,280254	0,820064	10,8	3,606668

$$I_y = \frac{\lambda_{\max} - n}{n-1} = \frac{8.49-4}{4-1} = 1,49,$$

$$B_y = \frac{I_y}{B_1} = \frac{0.149}{0.9} = 0,095.$$

$\lambda_{\max}$ – найбільше власне значення матриці парних порівнянь;

n – розмірність матриці;

B_1 – випадковий індекс.

Відношення узгодженості матриці відповідає умові, при якій матрицю вважаємо достатньо узгодженою, а саме воно не перевищує величини 0,1.

Проаналізувавши основні критерії за котрими проводилось дослідження, було виявлено, що основними критеріями котрі можуть захистити персональний комп'ютер користувача від методів соціальної інженерії є:

- автентифікація
- ідентифікація
- управління терміналом.

Просте, слід враховувати що важливою частиною цих критеріїв є:

- Складні паролі.
- Унікальні ідентифікатори.
- Автоматичне блокуваня облікового запису при неправильних спробах входу у ПК
- Використання двухфакторної автентифікація.
- Перехід в сплячий режим при бездіяльності ПК.

Контроль доступу до файлів був так низько оцінений експертами, через те, що якщо злодій вже має доступ до файлів, то зазвичай він має доступ и до самої системи.

Висновки

У ході проведення данного дослідженн було розглянуто методи захисту корпоративної мережі. Зібрано та проаналізовано інформацію з приводу політик безпеки. Проаналізовано поняття інфомаційної безпеки та основні принципи запобігання порушень безпеки. Проаналізовано поняття політики безпеки та проведено опитування з приводу найважливіших місць захисту.

Список літератури

1. Lytvynov V., Stoianov N., Skiter I., Trunova H., Hrebennyk A. Corporate Networks Protection Against Attacs Using Content-Analysis of Global Information Space. *Technical Sciences and Technologies*. 2018. № 1 (11). P.115-130. URL: DOI: 10.25140/2411-5363-2018-1(11)-115-130
2. Computer Science and Telecommunications Board System Security Study Committee. National Research Council (U.S.). National Academies Press.1990. 320 p.
3. Rosenberry T. Protecting Your Corporate Network from Your Employee's Home Systems. GIAC Security Essentials Certification. SANS Institute. 2020.
4. Sathyadevan S., Rangan V., Achuthan K. Security Layer and Methods for Protecting Tenant Data in a Cloud-Mediated Computing Network. *Patent Application Publication*. 2014. 17 p.
5. Shamuhamedov G., Hydyrov N. Security and protection of information in networks. *Technical Sciences.* URL: https://cyberleninka.ru/article/n/security-and-protection-of-information-in-networks/pdf

PROTECTION OF CORPORATE NETWORKS FROM HUMAN INFLUENCE USING TECHNICAL MEANS

Y. Tkach[1], O. Yakovlev[2], T. Lisitsa[2]

[1]National Chernihiv Polytechnic University
Shevchenko 95, Chernihiv, Ukraine, E-mail: tkachym79@gmail.com
[2]JSC "Alfa-Bank". Ave. Victory, 62. Chernihiv, Ukraine, Email: samehada@i.ua

The widespread use of computer technology in automated data processing and management systems has exacerbated the problem of protecting information circulating in computer systems from unauthorized access. Information protection in computer systems has a number of specific features due to the fact that information that is not strictly related to the media can be easily and quickly copied and transmitted over communication channels. In computer networks, targeted information belongs to certain people who are on their own initiative or in accordance with official responsibilities, and only they have the right to use this information. Such information should be protected from all forms of external interference, especially from the reading and copying of this information, by people who do not have the right to access this information. The aim of the work is to study the methods of corporate network protection, collection and analysis of information on security policies. Therefore, a survey was conducted among experts to identify the most important points in technical protection that can be used against the methods of social engineering. To do this, the results of the survey were analyzed and the main criteria were selected. Next, using the matrix of preferences and mathematical analysis, it was identified which of the selected criteria are the most important, and identified factors that can both positively and negatively affect the selected basic criteria. This is necessary in order to understand exactly how you can protect yourself from the methods of social engineering.

Keywords: information security; human factor; security policy; authentication; identification; access control.