УДК 351.746
DOI https://doi.org/10.37687/2413-6433.2020-2.13

Шепета О.В.,
кандидат юридичних наук, доцент,
доцент кафедри організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України
ORCID: 0000-0002-8485-0349

Тугарова О.К.,
кандидат юридичних наук, доцент,
доцент кафедри організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України
ORCID: 0000-0003-1346-8342

ПРИВІЛЕЙОВАНІ ОБЛІКОВІ ЗАПИСИ ЯК КЛЮЧОВИЙ АСПЕКТ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

PRIVILEGED ACCOUNTS AS A KEY ASPECT OF INFORMATION SECURITY SYSTEMS

Стаття присвячена аналізу огляду питання захисту інформації в інформаційно-телекомунікаційних системах (ІТКС) та визначенню ролі облікових записів, оскільки саме вони є основним найпростішим способом дістатися інформації з обмеженим доступом. Викрадення облікових даних є найпростішим способом отримати доступ до інформації з обмеженим доступом, тому що дані облікових записів знають 2 суб'єкта (здебільшого): особа, яка використовує обліковий запис, та система, в якій цей обліковий запис створено. Оскільки система, в якій зберігається обліковий запис, є, скоріш за все, комп'ютерною системою, використання уразливості системи є єдиним способом отримати інформацію облікового запису, а оскільки технології щодня покращуються, таких вразливостей щодня стає дедалі менше. Для захисту від реальних та потенційних загроз в інформаційно-телекомунікаційних системах реалізовують функції захисту, які в сукупності створюють так звані послуги безпеки. Кожна послуга, яка складається з набору функцій, протистоїть певній множині загроз конфіденційності, цілісності, доступності чи спостережуваності. На відміну від комп'ютерної системи, людина більш уразлива до внутрішніх та зовнішніх загроз, що можуть вплинути на неї з метою отримання необхідної інформації, саме тому здебільшого саме людина стає об'єктом впливу зловмисників із метою отримати доступ до облікового запису, після чого доступу до системи обробки інформації, наприкінці – отримання доступу до інформації з обмеженим доступом. Зазначено, що досліджувана проблематика стає ще більш актуальною у зв'язку з розширенням використання комп'ютерних систем для обробки інформації з обмеженим доступом. Дослідженням цієї проблеми здебільшого займаються за кордоном співробітники компаній, що опікуються інформаційною безпекою. В Україні захистом облікових записів частіш за все займаються ті компанії, що є партнерами іноземних компаній, як приклад, банк Raiffeisen. Однією з перших власне українських компаній, що серйозно поставилась до захисту облікових записів, стала компанія Київстар: однією з перших в Україні вона впровадила систему захисту привілейованих облікових записів CyberArk. Це дало змогу не тільки забезпечити максимальний рівень зберігання та захисту даних облікових записів, але й додатково безпечно та контрольовано надавати доступ до внутрішньої системи зовнішнім підрядникам та відслідковувати всі їхні дії.

Ключові слова: *інформаційна безпека, облікові записи, привілейовані облікові записи, захист інформації, CyberArk, система керування привілейованими обліковими записами, система управління привілейованими обліковими записами, аккаунти, привілейовані аккаунти.*

The article focuses on analyzing the overview of information security in information and telecommunication systems (ITCS) and identifying the role of accounts in this matter, since accounts are the single simplest way to gain access to restricted information. Theft of credentials is the easiest way to access restricted information because account data is known by 2 entities (in most cases) – the person using the account and the system in which the account was created. Since the system on which the account is stored is most likely a computer system, exploiting the vulnerability of the system is the only way to obtain account information, and as technologies improve every day, these vulnerabilities become less and less frequent. To protect against real and potential threats, information and telecommunication systems implement protection functions, which together create so-called security services. Each service, which consists of a set of features, confronts a number of threats to confidentiality,

integrity, accessibility or observability Unlike a computer system, a person is more vulnerable to being exposed to inner and outward threats which is why, in most cases, it is the person who becomes the target of the attackers in order to gain access to the account, and then gain access to the system end-to-end information processing – access to restricted information. It is noted that the issue is becoming more relevant in view of the increased use of computer systems to handle restricted information. In most cases, the study of this problem is carried out abroad and the employees of companies engaged in information security are engaged in the research. In Ukraine, the issue of account protection is most often addressed by companies that are partners with foreign companies, as an example of Raiffeisen Bank. One of the first Ukrainian companies to take account protection seriously was Kyivstar; they were among the first in Ukraine to introduce a CyberArk privileged account security system. This not only provided the maximum level of account data storage, but also additionally enabled the keeping and securing controllable access of the internal system to external contractors and kept track of all their activities.

Key words: *information security, accounts, privileged accounts, privileged accounts protection, securing privileged accounts, privileged account management solution, PAM.*

Постановка проблеми. Сучасний світ переходить до етапу, коли інформація стає найбільшою цінністю. Щодня можна почути, побачити, прочитати новину, в якій буде сказано, що компанія зазнала втрат через вірусну атаку, що призупинила роботу інформаційно-телекомунікаційних систем підприємства (ІТКС), або новину, що в мережі Інтернет з'явились сотні тисяч особистих даних клієнтів певної компанії, а особисті дані – це тип конфіденційної інформації, і полювання за такого типу інформацією або за іншого роду інформацією (комерційною таємницею, службовою інформацією і т.д.) ведеться щодня.

Витік інформації з обмеженим доступом відбувається щодня, це можуть бути хакерські атаки ззовні або робота інсайдерів із компанії, а особливо важливо те, що більшість таких атак (80%) [1] виконується з використанням облікових записів.

Мабуть, ви неодноразово отримували незрозумілі СМС на ваш мобільний номер, де вказувалось ваше ім'я та інформація, що ви виграли приз або берете участь в якомусь розіграші і т.д. Прикладів може бути дуже багато, але всі вони вказують, що ваші особисті дані були передані третій особі за вашою згодою або без неї.

Метою роботи є розкриття змісту понять привілейованих облікових записів та визначення їх місця в процесі викрадення інформації.

Об'єктом роботи є привілейовані облікові записи як ключовий момент у процесі викрадення інформації.

Предметом роботи є способи забезпечення безпеки привілейованих облікових записів.

Виклад основного матеріалу. Обліковий запис у комп'ютерній системі – сукупність наданої інформації про користувача, засобів та прав користувача щодо багатокористувацької системи [2]. Облікові записи (ОЗ) можна поділити на 2 групи: непривілейовані та привілейовані.

Непривілейовані облікові записи – тип облікового запису, що має мінімальний набір привілеїв, що дозволяють користувачеві лише війти в систему та переглядати інформацію, доступ до якої йому потрібен, всі інші дії для такого типу облікового запису є недоступними. Прикладами такого типу облікових записів можуть бути такі облікові записи в ОС Windows:

1) Гість;
2) Guest;
3) Інші облікові записи, створені не для адміністративних дій.

Такі облікові записи є майже в кожного працівника будь-якої компанії незалежно від посади, обов'язків тощо; використовуючи такі облікові записи, особа може автентифікуватися на будь-якому комп'ютері в мережі компанії та виконувати свою роботу без змоги вносити зміни в налаштування комп'ютера або налаштування інших комп'ютерів у мережі.

Привілейований обліковий запис – це обліковий запис користувача, який має більше привілеїв, ніж звичайні користувачі. Привілейовані облікові записи дають змогу, наприклад, встановити або видалити програмне забезпечення, оновити операційну систему або змінити конфігурації системи чи програми. Вони також можуть мати доступ до файлів, які зазвичай не доступні звичайним користувачам [3]. Такі облікові записи найчастіше перебувають у групах:

1) Адміністратори;
2) Доменні адміністратори;
3) Admins;
4) Domain Admins.

Привілейовані облікові записи можуть бути використані для різного роду зловмисних діянь: від викрадення доступних даних до створення умов для викрадення або витоку даних, які не доступні для певного користувача, але це буде можна змінити.

Особливу увагу треба приділяти привілейованим обліковим записам, оскільки саме користувачі з підвищеним рівнем привілеїв мають більше можливостей викрасти інформацію, що має певну цінність. До таких користувачів можна зарахувати:

1) адміністраторів ІТКС;
2) менеджерів вищого рівня;
3) керівників відділів.

Саме ці особи найчастіше мають привілейовані ОЗ та є основними цілями зловмисників. Крім того, що ці особи, а саме їх ОЗ, є цілями для зловмисників, вони самі можуть бути інсайдерами, котрі викрадають інформацію та незаконно її використовують.

Як вже було сказано в попередньому розділі, привілейовані облікові записи є небезпечними для підприємства та несуть найбільшу небезпеку для ІТКС підприємства. Тому постає питання порядку використання та захисту такого типу облікових записів.

Оскільки обліковий запис сам себе захистити не може, його має захищати та особа, котра його використовує, та організація, якій цей привілейований ОЗ належить. Далі ми розглянемо, які дії для захисту має вжити особа, яка використовує привілейований ОЗ для недопущення його використання третіми особами, та дії, які треба вжити підприємству для недопущення втрати привілейованого ОЗ і можливості його незаконного використання.

Особа, яка використовує обліковий запис для недопущення його втрати, має:

1) забезпечити надійний пароль до ОЗ;

2) забезпечити конфіденційність паролю та облікових даних;

3) не запускати підозрілих програм на робочому комп'ютері з правами свого привілейованого ОЗ;

4) не переходити за підозрілими посиланнями;

5) не вводити облікові дані від привілейованого запису на ресурсах, що не є ресурсами організації, в якій був створений цей ОЗ.

Організація, чий привілейований ОЗ використовує особа, має забезпечити:

1) максимальний рівень безпеки збереження облікових даних;

2) безпечні канали передачі даних;

3) неможливість потрапити в мережу організації ззовні без реальної на то необхідності;

4) високий рівень перевірки всіх файлів, що потрапляють у мережу;

5) навчання користувачів роботи з обліковими записами;

6) політики регулярної зміни паролів до ОЗ;

7) політики забезпечення комплексності паролю;

8) впровадження систем керування привілейованими обліковими записами (pam рішень).

Максимальний рівень безпеки збереження облікових даних забезпечується шляхом проведення постійних тренінгів та лекцій, на котрих співробітникам мають пояснювати, що не треба зберігати облікові дані у відкритих файлах на комп'ютері або записувати на папірці, котрий лежить на робочому столі працівника.

Проведення такого роду лекцій та тренінгів знизить можливість витоку облікових даних за межі вашої організації, оскільки часто можна побачити, що в невеликих організаціях облікові записи працівники передають іншим працівникам за допомогою месенджерів для виконання певної роботи. В умовах сучасності це недопустимо з великої кількості причин. По-перше, передаючи свої облікові дані третій особі, не можна простежити, хто вчинив певне діяння, оскільки дії вчинені від вашого облікового запису, але не вами. По-друге, передаючи облікові дані через мережу Інтернет, треба бути впевненим у каналах передачі даних, оскільки із самих каналів передачі даних можна отримати облікові дані та використати їх у злочинних цілях. Тут ми плавно переходим до наступного пункту забезпечення безпеки облікового запису – безпечні канали передачі даних.

Безпечні канали передачі даних потрібні, щоб забезпечити безпечну передачу облікових даних через мережу від одного пристрою до іншого. Рекомендується передавати інформацію між пристроями лише в шифрованому вигляді. Залежно від важливості інформації, що передається каналами зв'язку, треба використовувати різні протоколи шифрування. Найновішим та найбільш надійним є протокол TLS 1.3. Також для безпечної передачі даних рекомендується використовувати канали передачі даних із захистом від витоку інформації технічними каналами, такими як побічні електромагнітні випромінювання тощо. Це зробить неможливим отримання інформації особами, що зчитують канали зв'язку в організації та перебувають у ній незаконно. Це підводить нас до наступного пункту – захист мережі організації ззовні без потреби на це.

Підключення до внутрішньої мережі ззовні є особливо важливим моментом у будь-якій організації, оскільки від цього не можна відмовитись у сучасних умовах, дедалі більше компаній наймають працівників з інших країн, вони під'єднуються до внутрішньої мережі ззовні, і це не єдина причина, з якої потрібне підключення у внутрішню мережу ззовні. Найяскравішим прикладом, коли великій кількості людей потрібен був віддалений доступ для виконання свої обов'язків, був спалах коронавірусу, котрий спричинив перехід на віддалену роботу чималої кількості людей. Для безпечного підключення треба використовувати надійні рішення, щоб будувати безпечні та надійні VPN-тунелі у внутрішню мережу та не допустять у внутрішню мережу осіб, що не повинні мати такого роду доступу. Крім побудови надійного тунелю, треба забезпечити перевірку особи, що використовує цей тунель, оскільки дуже часто тунель будується між пристроями і не можна перевіряти, хто його використовує, тому найкраще використовувати рішення, що змушують користувача пройти автентифікацію (краще 2-факторну або біометричну), – це забезпечить впевненість, що доступ був отриманий легітимно. Побудова надійного зовнішнього доступу захистить внутрішню мережу від неправомірних дій неавторизованих осіб, але не захистить від потрапляння в мережу загрозливих файлів. Це питання буде висвітлено далі.

Шкідливі файли є великою загрозою для організації, оскільки їх потрапляння може призвести

до непомітного витоку інформації без конкретної особи. Для захисту внутрішньої мережі можуть бути використані мережеві пастки, які є завідомо вразливими та спокушають шкідливий файл заразити цю систему. Після зараження пристрій, котрий був пасткою, сповістить співробітника про наявність такого файлу в мережі, що полегшить його пошук на інших пристроях у мережі. Крім того, в мережі встановлюються так звані «пісочниці», котрі перевіряють всі файли, що потраплять у мережу. Принцип роботи пісочниці такий: вона емулює різні види систем та запускає той чи інший файл, що прийшов з Інтернету, та слідкує за подальшими змінами в цих системах. За кілька хвилин така система може прокрутити десятки років роботи такого файлу та знайти той момент, коли та куди він звертався, або що хотів отримати. Крім того, йде перевірка вже з готовою базою даних вірусів, відомих у світі, і також такі системи використовують штучний інтелект для покращеного аналізу файлів. Ці всі пункти є надзвичайно важливими і забезпечують технічний захист інформації, але найбільш слабким місцем в організації є людина. Саме людина має емоції, почуття і т.д., це використовують зловмисники, але про це далі.

Для того щоб знизити ризик витоку облікових даних та інформації загалом від своїх співробітників, треба проводити постійні курси навчання та підвищення кваліфікації та пояснювати, що переходити за підозрілими посиланнями не потрібно, завантажувати картинки з котенятами, які надіслав на пошту хтось зі співробітників, теж не треба, використовувати особисту електронну пошту в робочих цілях не можна. Список того, що треба розповісти співробітникам, неповний, оскільки зловмисники теж розвиваються і шукають нові способи отримати те, що їм потрібно. Саме тому регулярні тренінги, масове просвітлення та постійні нагадування про наявні загрози знизить можливість витоку облікових даних, але просвітлення не врятує від підбору облікових даних і про це далі.

Регулярна заміна пароля є надзвичайно важливою, оскільки, знаючи ім'я та прізвище співробітника, можливо сформувати його логін та підібрати пароль за сформованим словником. Частіше за все використовуються стандартні паролі:

1) дата народження;
2) ім'я дитини/чоловіка/дружини;
3) значимі дати;
4) стандартні паролі за типом «qwerty».

Саме тому треба створювати надійні парольні політики та змушувати користувачів постійно міняти свої паролі. Але користувачі змінюють паролі не частіше ніж раз на місяць, частіша зміна паролів призводить до проблеми запам'ятовування, саме тому краще використовувати рішення класу PAM, котрі будуть автоматично керувати обліковими записами.

Особливу увагу треба приділити останньому пункту – впровадження систем керування привілейованими обліковими записами. Це є вкрай необхідним, оскільки впровадження такої системи дасть змогу:

– забезпечити максимальний рівень безпеки збереження облікових даних;

– знизити ризики в разі оформлення доступу для зовнішніх користувачів;

– забезпечити регулярну та часту зміну паролів до ОЗ;

– забезпечити максимальній рівень складності паролю;

– контролювати дії користувачів під час сесії з привілейованим ОЗ.

У наступному розділі ми більш детально розглянемо можливості систем керування привілейованими обліковими записами та визначимо світових лідерів у цій сфері.

Найбільшою світовою компанією, що проводить аналіз ринку в області інформаційної безпеки, є компанія Gartner. Відповідно до звітів аналітичної компанії Gartner за 2018 рік, останнього офіційного аналітичного звіту ринку PAM (Privileged Account Management), лідером цього ринку стало рішення компанії CyberArk.

CyberArk є найкращим виробником програмних продуктів класу PAM, а саме CyberArk Privileged Access Security. Найголовнішими функціями цього рішення є:

– можливість щоденної заміни паролю;

– змога сформувати пароль будь-якої складності до 256 символів;

– змога зберігати облікові данні в захищеному виді (зберігання з 3-рівневим шифруванням даних);

– змога встановлювати захищені сесії між користувачем та цільовою системою (ЦС), не розкриваючи паролю користувачеві;

– змога вести повний відео- та текстовий запис сесії;

– можливість автоматичного реагування на дії користувача (детектування, призупинення сесії або розірвання сесії);

– автоматичне повідомлення співробітників безпеки в разі небезпечних ситуацій;

– можливість інтеграції з будь якими системами;

– можливість використання 2-факторної автентифікації;

Це не вичерпний перелік всіх функцій цього рішення, а лише основні, які допоможуть організації забезпечити максимальний рівень безпеки та попередити незаконне використання привілейованих облікових записів, що може призвести до непередбачуваних наслідків.

Висновки. Отже, облікові записи є важливою частиною будь-якої організації, але найбільшу увагу треба приділяти привілейованим обліковим записам, що частіше стають ціллю зловмис-

ників та потім використовуються у 80% посягань на ІТКС організацій.

Захистом цих привілейованих ОЗ мають займатись особи, що ними користуються, та організація, чиєю власністю є облікові записи. Особи, що користуються обліковими записами, мають вживати усіх заходів для того, щоб облікові дані не були втрачені з їх вини. З боку підприємства найбільш дієвим заходом буде впровадження системи управління привілейованими обліковими записами, що зможе створити максимальний рівень безпеки для збереження привілейованих ОЗ.

Найкращим рішенням ринку рішень класу PAM є рішення CyberArk Privileged Account Security, саме воно, за звітом аналітичної компанії Gartner, має найбільший функціонал у роботі з привілейованими обліковими записами та забезпечує найвищий рівень їх зберігання.

Список використаних джерел:

1. Avanessian A. The Perils of Full Administrator Rights. 2019. URL: https://www.infosecurity-magazine.com/blogs/perils-full-administrator-rights/ (дата звернення: 17.08.2020).

2. Обліковий запис : Wikipedia. 2014. URL: https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81 (дата звернення: 17.08.2020).

3. Privileged Account. 2017. URL: https://www.ssh.com/iam/user/privileged-account (дата звернення: 17.08.2020).