СЛУЖБА БЕЗПЕКИ УКРАЇНИ
Головне управління Служби безпеки України в Донецькій та Луганській областях
2 управління (з дислокацією у м. Маріуполь Донецької області)
вул. Архітектора Нільсена, 33, м. Маріуполь, Донецька область, 87515, тел. (0629) 52-53-94
www.ssu.gov.ua, e-mail: usbu_mariupol@ssu.gov.ua. Код ЄДРПОУ 20001504

08.02.22 № 18/2/41-вих-21 На № _____ від _____

Начальнику Департаменту охорони здоров'я Донецької обласної державної адміністрації
Володимиру КОЛЕСНИКУ
84313, Донецька область, м. Краматорськ, вул. Богдана Хмельницького, 6

Шановний пане Володимире!

2 управлінням ГУ в рамках визначеної законодавством компетенції здійснюються заходи щодо забезпечення безпеки функціонування державних інформаційних ресурсів, захисту національного кіберпростору від шпигунських, диверсійних, терористичних посягань, кіберрозвідок іноземних держав, кібертерористів і кіберзлочинців.

У ході виконання зазначених заходів, фіксуються факти загострення загрози національній безпеці України, спричинених протиправною діяльністю у кіберпросторі іноземних спецслужб, організацій та окремих осіб, а саме заходи кібернетичного впливу на державні установи та органи місцевого самоврядування з метою ураження комп'ютерних мереж і ПЕОМ співробітників для отримання віддаленого доступу, спотворення, знищення або викрадення службової інформації.

З урахуванням фіксації акцій кібернетичного впливу зі сторони російських спецслужб із залученням підконтрольних їм хакерських угрупувань на інформаційно-телекомунікаційні системи органів державної влади України та об'єктів критичної інфраструктури, для посилення рівня інформаційної безпеки та нейтралізації кіберзагроз, СБУ розроблені типові рекомендації з кіберзахисту. Враховуючи вищевикладене, пропонуємо вжити першочергових заходів реагування та доведення до підлеглих співробітників, відповідальних за технічний захист інформації, основні рекомендації щодо першочергових заходів з кіберзахисту (додається).

Додатково, з метою отримання об'єктивної інформації стосовно складу та захищеності власних інформаційно-телекомунікаційних систем, просимо здійснити

внутрішню інвентаризацію та надати інформацію згідно встановленого алгоритму (додається).

У зв'язку із службовою необхідністю відповідь просимо надати в стислі терміни.

Додаток:

1. *Алгоритм проведення інвентаризації наявних апаратних та програмних засобів на 4 (чотирьох) аркушах, не таємно.*
2. *Рекомендації щодо першочергових заходів з кіберзахисту на 8 (восьми) аркушах, не таємно*

З повагою,
Т.в.о. першого заступника начальника ГУ-начальника 2 управління **Денис ВАЛЕНТЮК**

Виконав: Присяжнюк Д.І.
380978487528

Додаток №1

АЛГОРИТМ

проведення інвентаризації наявних апаратних та програмних засобів, що використовуються в інформаційно-телекомунікаційних системах органів державної влади та підприємств, що перебувають у сфері їх управління.

З метою побудови належного рівня кіберзахисту інформаційно-телекомунікаційних систем органів державної влади необхідно:

1. Провести аудит наявного програмного та апаратного забезпечення, засобів захисту, що використовується для роботи сервісів (мережеве/серверне обладнання, тощо) та заповнити таблицю (додаток 1).

2. Провести аудит клієнтського сегменту мережі (робочі станції, ноутбуки, мережеві пристрої, тощо) та наявних публічних IP-адрес, заповнити таблицю (додаток 2) та надати додаткову інформацію щодо забезпечення:

- логування (надати інформацію про використання централізованого рішення щодо збору журналів подій, використання системи управління інформаційними подіями (SIEM) та зазначити період ведення журналів);
- безпеки (надати інформацію щодо захисту хостів та мережі, вказати інформацію про інциденти, що призвели до втрати інформації або порушень у роботі сервісів за 2020 рік);
- сканування вразливостей (надати інформацію про факти проведення сканування мережі на вразливості та вжиті заходи).

3. Побудувати топологію мережі із зазначенням фізичних та логічних зв'язків, IP-адрес, сегментів мережевої інфраструктури, ключового мережевого/серверного обладнання та засобів захисту.

(Зразок)

Програмне та апаратне забезпечення, засоби захисту, що використовується для роботи сервісів

№ п/п	Тип[1]	Виробник, модель, операційна система	Вид постачання[2]	Розміщення, відповідальні адміністратори, можливість віддаленого адміністрування[3]	Сервіси, та встановлене програмне забезпечення, наявність КСЗІ/СУІБ[4]	Інформація про сервіс[5]	Засоби захисту[6]	Розробка та супроводження сервісу[7]
1.	Маршрутизатор	Cisco ASA 5505, FX OS	Державна закупівля	Внутрішнє, Внутрішні, SSH	Внутрішня мережа, побудовано КСЗІ	192.168.100.50	NGFW	Власна розробка
2.	Сервер	Dell 3750, Windows Server 2016	Державна закупівля	Внутрішнє, Внутрішні, RDP	Контролер домену, Файловий сервер, Active Directory, DFS, КСЗІ не побудовано	10.15.20.25, AD1.gov.local	Антивірус, DLP, FW	Власна розробка
3.	Сервер	HP HPE DL20 Gen9 2LFF, Ubuntu 18.04	Благодійна допомога (отримано від НАТО)	Зовнішнє (ТОВ «ВЕБ-компані»), Зовнішні (ТОВ «ВЕБ-компані»), OpenVPN	Веб сайт «www.info.gov.ua», Apache HTTP Server, побудовано КСЗІ	100.80.221.25, 10.15.20.100, info1.gov.local	WAF, NGFW	Замовлення, ТОВ «ВЕБ-компані», наявний адміністративний доступ
4.	Віртуальний сервер	VMware ESXi 6.5, Windows Server 2019	Державна закупівля	Внутрішнє, Внутрішні, RDP	Сервіс електронної пошти, Microsoft Exchange 2019, КСЗІ не побудовано	172.10.15.20, mail.gov.local	Антивірус, Mail Gateway, NGFW	Власна розробка

[1] Необхідно вказувати фізичні та віртуальні сервери, мережеве обладнання, дискові сховища (у т.ч. файлові ресурси спільного використання)

[2] Вказати джерело надходження, для апаратного забезпечення отриманого від сторонніх організацій вказати у рамках чого та від кого отримано

[3] Вказати де фізично розташоване обладнання («внутрішнє» у випадку коли розташовано на території органу влади або підприємства, «зовнішнє» - вказати назву організації де встановлено), вказати хто здійснює його адміністрування («внутрішнє», якщо адміністрування здійснюють штатні співробітники, «зовнішнє» - вказати назву організації, яка адмініструє), можливість адміністрування з мережі Internet та спосіб підключення (VPN, SSH, TeamViewer, тощо)

[4] Вказати назву сервісу та все встановлене програмне забезпечення (у тому числі версії), наявність атестованої КСЗІ/СУІБ (вказати номер та дату)

[5] Вказати зовнішню/внутрішню IP-адресу, доменне ім`я

[6] Вказати всі засоби захисту сервісу, їх повну назву та модель/версію

[7] Вказати інформацію про розробника сервісу («власна розробка» якщо сервіс розроблявся органом влади або підприємством, «замовлення» - вказати назву організації, яка розробляла, а також інформацію про наявність адміністративного доступу)

Клієнтський сегмент мережевої інфраструктури, та додаткова інформація

Загальні питання	
Загальна кількість робочих станцій.	
Типи операційних систем, їх версія та кількість.	
Програмне забезпечення, що використовується, його версії, наявність ліцензії.	
Програмне забезпечення, що отримане від сторонніх організацій на безоплатній основі. Вказати від кого отримано та де використовується.	
Наявність можливості віддаленого підключення до робочих станцій.	
Вказати інформацію про засоби централізованого управління та контролю за станом робочих станцій (наприклад Microsoft AD, WSUS, SCCM, тощо).	
Логування	
Вказати інформацію про засоби централізованого збору та збереження журналів подій інформаційної безпеки, типи подій та з яких пристроїв.	

Вказати інформацію про використання системи управління інформаційними подіями (SIEM).	
Забезпечення безпеки	
Вказати інформацію про апаратні та програмні засоби захисту робочих станцій.	
Вказати інформацію про інциденти, що призвели до втрати інформації/порушень роботи ІТС/сервісів протягом 2020 року.	
Вказати інформацію про політику використання зовнішніх носіїв інформації (флеш-накопичувачі, зовнішні диски, тощо).	
Вказати інформацію про проведення аудиту безпеки (оцінки стану захищеності, перевірки дотримання вимог ТЗІ, тощо).	
Сканування вразливостей	
Вказати інформацію про факти проведення сканування мережі на вразливості та вжиті за результатами заходи.	
Публічні IP-адреси	
Вказати інформацію про публічні IP-адреси, що використовуються організацією, а також провайдерів що надають таку послугу.	

Додаток №2

РЕКОМЕНДАЦІЇ
щодо першочергових заходів з кіберзахисту

Рекомендації з підвищення рівня безпеки веб-ресурсів

1. Використання протоколів HTTPS та своєчасне оновлення SSL-сертифікатів.

використання протоколу HTTPS забезпечує цілісність і конфіденційність взаємодії з сервером, захищає дані користувачів при передачі в мережі Інтернет.

Налаштувати на веб-сервері примусове перенаправлення з HTTP на HTTPS.

2. Своєчасне оновлення програмного забезпечення починаючи з операційної системи та веб-сервера, закінчуючи фреймворком (якщо такий має місце) та окремими модулями.

3. Вимкнути можливість індексації та перегляду директорій веб-ресурсу.

Дані обмеження можна організувати за допомогою конфігурації веб-серверу, файлів .htaccess, для деяких випадків – розподілом прав доступу.

4. Налаштувати періодичне створення резервних копій.

Для створення можливості швидкого відновлення роботи ресурсу у критичних ситуаціях, база даних та файли сайту повинні зберігатись з однаковою частотою для уникнення колізій в роботі фреймворку та/або окремих модулів сайту (зберігати резервні копії в директоріях веб-ресурсу, не рекомендовано, використовуйте для цього окремі сховища).

5. Провести та налаштувати сегментацію мережевої інфраструктури з обов'язковим розмежуванням користувацької та серверної ланок, з обов'язковою взаємодією між ними через міжмережевий екрани (розміщувати веб-ресурси та інші сервіси призначені для обробки запитів користувачів в DMZ зоні). Заборонити доступ до панелі адміністрування веб-серверу з мережі Інтернет. Вимкнути сервіси та заблокувати порти, що не використовуються. Ввести двофакторну аутентифікацію (як мінімум для адміністраторів веб-ресурсу). Використовуйте захищені методи доступу до серверу для передачі файлів і управління ним (SFTP, SSH та ін.). При віддаленому адмініструванні через SSH заборонити авторизацію з правами ROOT, використовувати ключі (authorized_key). Змінити стандартний номер 22 SSH порту. Налаштуйте фільтрацію вхідних даних у веб-формах авторизації або у веб-формах додавання/зміни даних.

5. Встановити та налаштувати Next Generation Firewall, Web Application Firewall та рішення Anti-DDoS, в залежності від існуючої в організації потреби для покращення захисту веб-ресурсів мережевої інфраструктури.

6. Увімкнути всі можливі варіанти логування подій, реалізувати їх моніторинг та збереження на окремому дисковому сховищі (не менше 3 місяців).

7. Коректно налаштувати та постійно актуалізувати А-записи веб-ресурсів на DNS-сервері, оскільки DNS є важливою складовою доступності мережевих сервісів необхідно використовувати принаймні 2 (Master, Slave). У разі використання DNS-серверу провайдера з доступом до адміністративної панелі налаштувань необхідно періодично змінювати пароль доступу та надійно його зберігати, налаштувати доступ до панелі керування з визначеного переліку IP-адрес.

8. Періодична перевірка директорій на сервері веб-ресурсу з метою виявлення підозрілих файлів (пошук вебшелів).

Зазвичай в ході атак на сервері розміщують бекдори (вебшели) для віддаленого доступу до серверу сайту. Рекомендуємо періодично переглядати директорії веб-ресурсу для пошуку таких бекдорів. Для цього можливо

використовувати спеціальні скрипти або перевіряти наявність нових файлів в директоріях. Виявлення створеного сторонніми особами файлами буде свідчити про злам веб-ресурсу та можливості для подальших дій з пошуку вразливостей і їх експлуатації.

Часто відбувається зміна атрибутів файлів (не плутати з правами доступу) для заборони їх видалення та модифікації. Такі файли можна знайти за ідентифікатором immutable..

9. Управління правами доступу.

Налаштуйте дозволи для файлів та каталогів. Розподіляйте права доступу до файлів на сервері та окремих розділів сайту відповідно до завдань користувачів.

Доцільно розмежувати розташування скриптів та програм, даних, призначених тільки для читання, та даних, призначених для зміни відвідувачами.

10. Уникайте помилок конфігурацій серверу.

Обмежуйте доступ та/або видаляйте файли, які не використовуються сервером для роботи, але мають інформацію про сервер (наприклад phpinfo.php, temp.php, test.php), вимикайте та/або обмежуйте доступ до функціоналу серверу, який не використовується сервером для роботи, але надає інформацію про сервер (наприклад директива Apache «ExtendedStatus»).

11. Розміщуйте веб-ресурси на окремих веб-серверах. Для тестового середовища (тестові сервіси/додатки) використовувати окремий сегмент мережі.

Компрометація одного з веб-ресурсів на веб-сервері може призвести до компрометації всіх веб-ресурсів на ньому.

Крім того, бажано уникати розташування поштового серверу на сервері з веб-ресурсом.

12. Зберігайте лог-файли веб-серверу та системи у визначеному для цього місцях (уникайте зберігання лог-файлів в директоріях веб-ресурсу).

13. У веб-ресурсах що використовують CMS Wordpress заборонити доступ з мережі Інтернет до /xmlrpc.php, /wp-json/wp/v2/users, /wp-admin, /admin, /login, /wp-login.

14. Вимагати від розробників реалізації Content Security Policy або реалізувати самостійно.

Рекомендації з підвищення рівня безпеки поштового сервісу

1. Налаштувати SPF запис, який дозволятиме здійснювати перевірку відправника та уникнути його підробки (http://open-spf.org).

2. Налаштувати роботу технології DKIM, яка забезпечує метод валідації доменного імені відправника шляхом додавання до електронного листа цифрового підпису, який пов'язано із доменом відправника (http://dkim.org).

3. Впровадити політику комплексної перевірки відправника електронного листа DMARC, яка опирається на роботу SPF та DKIM (https://dmarc.org).

Важливим є впровадження технологій як на перевірку вхідної кореспонденції, так і на відправку з метою надання можливості її перевірки іншими суб'єктами, що отримують електронні поштові листи від імені відповідного державного органу.

Застосування технологій SPF, DKIM та DMARK є загальноприйнятою світовою практикою

За можливості пропонуємо впровадити технологію посилення захисту Web ресурсів – DNSSEC, яка забезпечує аутентифікацію даних DNS та дозволяє встановити факт несанкціонованої зміни змісту DNS відповіді.

Разом із тим, в перспективі з метою забезпечення захисту від атак необхідно використовувати наступні сучасні рішення захисту, які відповідають за певний вектор атак, а саме:

1. Next Generation Firewall (NGFW) – міжмережевий екран нового покоління для виявлення аномалій в поштових протоколах та захисту платформи на якій працює поштова система.

2. Mail Security Gateway – поштовий шлюз, що забезпечує фільтрацію поштового трафіку та блокування зловмисної активності: спаму, вірусів тощо.

3. Web Application Firewall (WAF) – екран для публікації ВЕБ-інтерфейсу користувача до мережі Інтернет.

4. Anti-Virus – агент, що встановлюється на сервери та забезпечує захист ОС на якій побудована поштова система.

5. Sandbox – пристрій для емуляції загроз в ізольованому середовищі, виконує аналіз потенційно небезпечних файлів в поштовому трафіку.

Важливо! У разі наявності ресурсів, доступ до яких має бути забезпечено з мережі Інтернет, важливим аспектом їх доступності є захист від DDoS-атак, які спрямовані на відмову в обслуговуванні. Таким чином, доцільним є використання систем анти-DDoS на рівні оператора/провайдера телекомунікацій, що надає доступ до мережі Інтернет.

Рекомендації з підвищення рівня безпеки корпоративної мережі

1. Впровадити SSHv3 (у разі неможливості, щонайменше SSHv2) або TLS (не нижче 1.2) для забезпечення безпечної комунікації при віддалених підключеннях до мережевих пристроїв, сервісів, серверного обладнання.

2. Заборонити використання у мережі протоколів: HTTP, FTP, Telnet, ICMP, SNMP, SMB (у разі необхідності застосування, використовуйте SNMPv3 разом із списком доступу Management Information Base (MIB), додаткова інформація https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/reducing-the-risk-of-snmp-abuse.cfm, а також HTTPS, SFTP, SMBv2 (та вище) інші протоколи, які підтримують TLS шифрування версії не нижче 1.2).

3. Вимкнути усі фізичні порти та інтерфейси мережевих пристроїв, що не використовуються для уникнення можливості несанкціонованих підключень.

4. Увімкнути функцію port security мережевих пристроїв, за наявності.

5. Фізично розмежувати користувацьку, адміністративну мережі із мережею підключення та управління мережевими пристроями. У разі неможливості максимально обмежити, за допомогою списків IP-адрес, з яких сегментів мережі можливий доступ до адміністративних панелей керування пристроями та сервісами.

6. Використовувати списки доступів із визначеними IP адресами для адміністративних підключень.

7. Заборонити функціонування будь-яких безпровідних точок доступу, відключити Wi-Fi маршрутизатори. Можливо дозволити (за необхідністю) функціонування (гостьових) безпровідних точок доступу наприклад в приміщенні прес-центру або кімнаті відпочинку, в такому випадку Wi-Fi маршрутизатор повинен знаходитись в окремій ізольованій підмережі з прямим підключенням до провайдера Інтернет послуг.

8. Максимально обмежити за допомогою списків доступу IP-адреси з яких можливий доступ до адміністративних панелей керування пристроями та сервісами.

9. Увімкнути логування подій (доступ до серверів, мережевих пристроїв, баз даних тощо), реалізувати їх моніторинг та збереження на окремому дисковому сховищі (не менше 3 місяців).

10. Використовувати вбудовані міжмережеві екрани та/або окремі VLAN для максимального обмеження можливості з'єднань робочих станцій та серверів одне з одним, щоб уникнути горизонтального просування у мережі у випадку компрометації її окремих вузлів або сегментів

11. Віддалене підключення до корпоративної мережі з домашніх пристроїв, службових пристроїв осіб, що перебувають у відрядженнях, в тому числі для заходів адміністрування, співробітників відокремлених підрозділів здійснюйте з використанням технології VPN (наприклад IPsec, L2TP). При цьому, запровадьте окремі облікові записи для кожного окремого користувача, двофакторну авторизацію, списки доступів вхідних IP-адрес та доступних IP-адрес, забезпечте ведення журналів підключень тощо.

12. Важливим аспектом забезпечення спостережності та контролю за мережею є моніторинг мережевого трафіку та роботи користувацького комп'ютерного обладнання, у зв'язку з чим в подальшому доцільним є налаштування Next Generation Firewall, систем захисту від вторгнень (IPS\IDS), які на основі правил здатні виявляти мережеві атаки, спроби несанкціонованого доступу, підвищення привілеїв, появи шкідливого ПЗ, відкриття нового порту, тощо. Іншим можливим шляхом виявлення ознак компрометації є використання SIEM систем, що на основі даних про роботу обладнання дасть можливість накопичувати та аналізувати події безпеки, виявляти в режимі реального часу атаки або аномальну поведінку в мережі та дозволить вчасно реагувати на кіберінциденти, за необхідності проводити розслідування кібератак.

13. Проводити регулярний аудит (внутрішній та зовнішній) з скануванням вразливостей (pentest).

Рекомендації з підвищення рівня безпеки комп'ютерів користувачів

1. Оновити/перевстановити застарілі операційні системи на сучасні версії з актуальними оновленнями (не нижче Windows 10). У разі неможливості встановлення ОС Windows 10 з технічних причин, в якості альтернативи використовувати ОС UALinux або інші операційні системи сертифіковані Державною службою спеціального зв'язку та захисту інформації України.

2. Використовувати лише ліцензійні програмні продукти. Заборонити використання так званих активаторів або зламувачів програмного забезпечення.

3. Створити перелік дозволеного ПЗ для використання на комп'ютерах користувачів, списки дозволених .exe, .com файлів, скриптів (e.g. .ps1, .bat, .cmd, .vbs and .js files), установщиків (e.g. .msi, ..msp and .mst files). Забезпечити їх постійну актуалізацію.

Встановлення будь-якого програмного забезпечення на комп'ютерах користувачів здійснювати виключно адміністратором.

4. Здійснювати регулярне резервне копіювання даних, зберігати резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштувати функцію «відновлення системи».

5. Регулярно актуалізувати список користувачів та здійснити розподіл доступу користувачів та адміністраторів мереж до необхідних сервісів та компонентів за попередньо визначеними групами та ролями.

6. Впровадження Microsoft AppLocker або Device Guard та GPO

(https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview)

(https://docs.microsoft.com/en-au/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control)

7. Впровадження Attack Surface Reduction для захисту Microsoft Office.

(https://docs.microsoft.com/en-au/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction)

- блокування виконуваних файлів з поштових листів
  BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550
- блокування створення Office від створення процесів
  D4F940AB-401B-4EFC-AADC-AD5F3C50688A
- блокування створення Office виконуваних файлів
  3B576869-A4EC-4529-8536-B80A7769E899
- блокування впровадження Office коду в інші процеси
  75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
- блокування JavaScript та VBScript від запуску виконуваних файлів
  D3E037E1-3EB8-44C8-A917-57927947596D
- блокування потенційно обфускованих скриптів
  5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
- блокування викликів Win32 API з макросів Office
  92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B

GPO для ASR Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\

Windows Defender Exploit Guard\Attack Surface Reduction

Configure Attack Surface Reduction rules

Enabled

Set the state for each ASR rule:

75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 1

3b576869-a4ec-4529-8536-b80a7769e899 1

d4f940ab-401b-4efc-aadc-ad5f3c50688a 1

92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B 1

5beb7efe-fd9a-4556-801d-275e5ffc04cc 1

d3e037e1-3eb8-44c8-a917-57927947596d 1

be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 1

8. Кешування облікових даних лише останньої авторизації, замість усіх за допомогою GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Interactive logon: Number of previous logons to cache (in case domain controller is not available) 1 logons

Network access: Do not allow storage of passwords and credentials for network authentication Enabled

9. Впровадження Controlled Folder Access - захищає дані від несанкціонованого доступу програм, за допомогою встановлення обмежень на директорії і можливості доступу до них лише дозволеним програмам

(https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders)

GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\

Windows Defender Exploit Guard\Controlled Folder Access

Configure allowed applications Enabled Enter the applications that should be trusted: <organisation defined>

Configure Controlled folder access Enabled Configure the guard my folders feature: Block

Configure protected folders Enabled Enter the folders that should be guarded: <organisation defined>

10. Впровадження захисту облікових даних користувача в операційній системі шляхом забезпечення безпечного механізму їх введення GPO:

Computer Configuration\Policies\Administrative Templates\System\Logon

Do not display network selection UI Enabled

Enumerate local users on domain-joined computers Disabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface

Do not display the password reveal button Enabled

Enumerate administrator accounts on elevation Disabled

Require trusted path for credential entry Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options

Disable or enable software Secure Attention Sequence Disabled

Sign-in last interactive user automatically after a system-initiated restart Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Interactive logon: Do not require CTRL+ALT+DEL Disabled

11. Впровадження механізму перешкоджання несанкціонованому підвищенню прав користувача за допомогою GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

User Account Control: Admin Approval Mode for the Built-in Administrator account Enabled

User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop Disabled

User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Prompt for credentials on the secure desktop

User Account Control: Behavior of the elevation prompt for standard users Prompt for credentials on the secure desktop

User Account Control: Detect application installations and prompt for elevation Enabled

User Account Control: Only elevate UIAccess applications that are installed in secure locations Enabled

User Account Control: Run all administrators in Admin Approval Mode Enabled

User Account Control: Switch to the secure desktop when prompting for elevation Enabled

User Account Control: Virtualize file and registry write failures to per-user locations Enabled

12. Блокування використання доменного акаунту із привілеями локального адміністратора для управління робочими станціями. Для цього необхідно відключити локального адміністратора за допомогою GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Accounts: Administrator account status Disabled

У разі неможливості повного відключення локального адміністратора, застосовувати унікальні паролі до кожного акаунту та User Account Control у випадках віддаленого підключення із такими правами. GPO:

Computer Configuration\Policies\Administrative Templates\MS Security Guide

Apply UAC restrictions to local accounts on network logons Enabled

13. Заборонити використання Internet Explorer, у разі можливості - видалити, у разі якщо є необхідність використання стандартного браузеру Windows, використовувати Microsoft Edge із такими налаштуваннями GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge

Allow Adobe Flash Disabled

Allow Developer Tools Disabled

Configure Do Not Track Enabled

Configure Password Manager Disabled

Configure Pop-up Blocker Enabled

Configure Windows Defender SmartScreen Enabled

Prevent access to the about:flags page in Microsoft Edge Enabled

Prevent bypassing Windows Defender SmartScreen prompts for files Enabled

Prevent bypassing Windows Defender SmartScreen prompts for sites Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Network Protection

Prevent users and apps from accessing dangerous websites Enabled Block

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Application Guard

Turn on Windows Defender Application Guard in Enterprise Mode Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Microsoft Edge

Configure Windows Defender SmartScreen Enabled

Prevent bypassing Windows Defender SmartScreen prompts for sites Enabled

14. Використовувати наступні GPO для регулярного оновлення операційних систем (рекомендовано використовувати службу контролеру домену WSUS):

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update

Allow Automatic Updates immediate installation Enabled

Configure Automatic Updates Enabled

Configure automatic updating: 4 - Auto download and schedule the install

Schedule install day: 0 - Every day

Install updates for other Microsoft products

Do not include drivers with Windows Updates Disabled

No auto-restart with logged on users for scheduled automatic updates installations Enabled

Remove access to use all Windows Update features Disabled

Turn on recommended updates via Automatic Updates Enabled

15. Запровадити обов'язкове використання складних паролів для облікових записів користувачів (більше 8 символів, обов'язково: не менше однієї цифри, великої літери, спецсимволу). Заборонити порожні паролі. GPO:

Computer Configuration\Policies\Administrative Templates\System\Logon

Turn off picture password sign-in Enabled

Turn on convenience PIN sign-in Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy

Maximum password age 90 days

Minimum password length 8 characters

Password must meet complexity requirements Enabled

Store passwords using reversible encryption Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Accounts: Limit local account use of blank passwords to console logon only Enabled

16. Впровадити блокування облікового запису на певний час (наприклад 15 хвилин) при певній кількості невдалих спроб заходу (наприклад 5) для уникнення перебору паролів зловмисниками. GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Account lockout duration 0

Account lockout threshold 5 invalid logon attempts

Reset account lockout counter after 15 minutes

17. Впровадити заборону використання анонімних користувачів під час спільного мережевого доступу. Використовуючи анонімного користувача зловмисник може зібрати інформацію про користувачів віддаленої системи, груп, списку спільних мережевих ресурсів, версії ОС, наявних патчів. GPO:

Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation

Enable insecure guest logons Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Network access: Allow anonymous SID/Name translation Disabled

Network access: Do not allow anonymous enumeration of SAM accounts Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares Enabled

Network access: Let Everyone permissions apply to anonymous users Disabled

Network access: Restrict anonymous access to Named Pipes and Shares Enabled

Network access: Restrict clients allowed to make remote calls to SAM O:BAG:BAD:(A::RC:::BA)

Network security: Allow Local System to use computer identity for NTLM Enabled

Network security: Allow LocalSystem NULL session fallback Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Access this computer from the network Administrators , Remote Desktop Users

Deny access to this computer from the network NT AUTHORITY\Local Account

18. Забезпечити обов'язкове використання антивірусного ПЗ. у разі відсутності корпоративного антивірусу, налаштувати вбудований Windows Defender оптимальним чином. GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus

Turn off Windows Defender Antivirus Disabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ MAPS

Configure local setting override for reporting to Microsoft MAPS Disabled

Configure the 'Block at First Sight' feature Enabled

Join Microsoft MAPS Enabled

Join Microsoft MAPS: Advanced MAPS

Send file samples when further analysis is required Enabled

Send file samples when further analysis is required: Send safe samples

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ MpEngine

Configure extended cloud check Enabled

Specify the extended cloud check time in seconds: 50

Select cloud protection level Enabled

Select cloud blocking level: High blocking level or High+ blocking level

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Quarantine

Configure removal of items from Quarantine folder Disabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Real-time Protection

Scan all downloaded files and attachments Enabled

Turn off real-time protection Disabled

Turn on behavior monitoring Enabled

Turn on process scanning whenever real-time protection is enabled Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\ Scan

Allow users to pause scan Disabled

Check for the latest virus and spyware definitions before running a scheduled scan Enabled

Scan archive files Enabled

Scan packed executables Enabled

Scan removable drives Enabled

Turn on e-mail scanning Enabled

Turn on heuristics Enabled

19. Запровадити механізм обов'язкового закріплення ідентифікатора зони (zone identifier) в операційній системі. Зловмисники можуть обходити механізми захисту операційної системи надсилаючи шкідливі вкладення у додатках до електронних листів у разі відсутності зазначених зон. GPO:

User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager

Do not preserve zone information in file attachments Disabled

Hide mechanisms to remove zone information Enabled

20. Забезпечити зберігання критично важливих подій у журналах операційних систем. GPO:

Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation
Include command line in process creation events Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application
Specify the maximum log file size (KB) Enabled
Maximum Log Size (KB): 65536
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security
Specify the maximum log file size (KB) Enabled
Maximum Log Size (KB): 2097152
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System
Specify the maximum log file size (KB) Enabled
Maximum Log Size (KB): 131072
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment
Manage auditing and security log Administrators
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit
Policies\Account Management
Audit Computer Account Management Success and Failure
Audit Other Account Management Events Success and Failure
Audit Security Group Management Success and Failure
Audit User Account Management Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit
Policies\Detailed Tracking
Audit Process Creation Success
Audit Process Termination Success
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit
Policies\Logon/Logoff
Audit Account Lockout Success
Audit Group Membership Success
Audit Logoff Success
Audit Logon Success and Failure
Audit Other Logon/Logoff Events Success and Failure
Audit Special Logon Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit
Policies\Object Access
Audit File Share Success and Failure
Audit File System Success and Failure
Audit Kernel Object Success and Failure
Audit Other Object Access Events Success and Failure
Audit Registry Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit
Policies\Policy Change
Audit Audit Policy Change Success and Failure
Audit Other Policy Change Events Success and Failure

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit

Policies\System

Audit System Integrity

Success and Failure

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Enabled

21. Заборонити автоматичне відкриття та запуск підключених носіїв даних. За допомогою автоматичного запуску, використовуючи файл autorun.inf зловмисники можуть використовувати переносні носії даних для зараження систем до яких вони були підключені. GPO:

Disallow Autoplay for non-volume devices Enabled

Set the default behavior for AutoRun Enabled. Default AutoRun Behavior: Do not execute any autorun commands

Turn off Autoplay Enabled. Turn off Autoplay on: All drives

22. Заборонити використання гостьових облікових записів. GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options Accounts: Guest account status Disabled

23. Заборонити користувачам доступ до консолі CMD. GPO:

User Configuration\Policies\Administrative Templates\System Prevent access to the command prompt Enabled. Disable the command prompt script processing also: Yes

24. Встановити заборону запису/запуску з портативних носіїв інформації. Зловмисники можуть розповсюджувати ШПЗ на переносних носіях даниих. GPO:

Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access

CD and DVD: Deny execute access Enabled

CD and DVD: Deny write access Enabled

Custom Classes: Deny write access Enabled

Floppy Drives: Deny execute access Enabled

Floppy Drives: Deny write access Enabled

Removable Disks: Deny execute access Enabled

Removable Disks: Deny write access Disabled

Tape Drives: Deny execute access Enabled

Tape Drives: Deny write access Enabled

WPD Devices: Deny write access Enabled

25. Обмежити використання спільних мережевих ресурсів та принтерів на комп`ютерах користувачів. GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup

Prevent the computer from joining a homegroup Enabled

User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing

Prevent users from sharing files within their profile Enabled

26. У разі запровадження доменних політик, пересвідчитись, що лише GPO застосовуються до робочої станції, а не локальні політики; пересвідчитись, що GPO не можуть бути локально змінені/відключені. GPO:

Computer Configuration\Policies\Administrative Templates\Network\Network Provider

Hardened UNC Paths Enabled, Hardened UNC Paths:*\SYSVOL, RequireMutualAuthentication=1, RequireIntegrity=1, *\NETLOGON, RequireMutualAuthentication=1, RequireIntegrity=1

Computer Configuration\Policies\Administrative Templates\System\Group Policy

Configure registry policy processing Enabled, Process even if the Group Policy objects have not changed

Configure security policy processing Enabled, Process even if the Group Policy objects have not changed

Turn off background refresh of Group Policy Disabled

Turn off Local Group Policy Objects processing Enabled

27. Обмежити можливість користувачів встановлювати програми. GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer

Configure Windows Defender SmartScreen Enabled

Pick one of the following settings: Warn and prevent bypass

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Explorer

Configure Windows Defender SmartScreen Enabled

Pick one of the following settings: Warn and prevent bypass

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer

Allow user control over installs Disabled

Always install with elevated privileges Disabled

User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer

Always install with elevated privileges Disabled

28. Заборонити автоматичний запуск програм разом із операційною системою. Зловмисники використовують планувальник завдань та гілки реєстру операційної системи для того щоб ШПЗ автоматично запускалось при старті ОС. Відключивши функцію автозапуску програм, доцільно визначити доменною політикою, які програми мають запускатись (Run these programs at user logon) та заборонити автозапуск інших.GPO:

Computer Configuration\Policies\Administrative Templates\System\Logon

Do not process the legacy run list Enabled

Do not process the run once list Enabled

29. Заборонити прив'язку акаунтів Макйрософт до локальних чи доменних профілів. Хоча це дозволяє переносити налаштування акаунту з комп'ютера на комп'ютер використовуючи OneDrive, це може призвести до витоку чутливої інформації. GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft account

Block all consumer Microsoft account user authentication Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive

Prevent the usage of OneDrive for file storage Enabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Accounts: Block Microsoft accounts Users can't add or log on with Microsoft accounts

30. Вимкнути NetBIOS over TCP/IP, який необхідний лише дял ОС молодше Windows 2000, проте має ряд вразливостей.

31. Використовувати для процедури аутентифікація протокол Kerberos та NTLMv2. GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Network security: Configure encryption types allowed for Kerberos AES128_HMAC_SHA1, AES256_HMAC_SHA1

Network security: LAN Manager authentication level Send NTLMv2 response only. Refuse LM & NTLM

Network security: Minimum session security for NTLM. SSP based (including secure RPC) clients Require NTLMv2 session security Require 128-bit encryption

Network security: Minimum session security for NTLM. SSP based (including secure RPC) servers Require NTLMv2 session security, Require 128-bit encryption

32. Вимкнути виконання скриптів та сценаріїв Powershell. GPO:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell

Turn on PowerShell Script Block Logging Enabled

Turn on Script Execution Enabled. Execution Policy: Allow only signed scripts

33. Заборонити програмам доступ до реєстру системи. GPO:

User Configuration\Policies\Administrative Templates\System

Prevent access to registry editing tools

Enabled, Disable regedit from running silently: Yes

34. Вимкнути remote assistance (відалений помічник). GPO:

Computer Configuration\Policies\Administrative Templates\System\Remote Assistance

Configure Offer Remote Assistance Disabled

Configure Solicited Remote Assistance Disabled

35. Заборонити використання вбудованого віддаленого підключення (remote desktop services)

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\

Remote Desktop Session Host\Connections

Allow users to connect remotely by using Remote Desktop Services Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Allow log on through Remote Desktop Services <blank>

У разі якщо неможливо відімкнути відалене підключення, обмежити підключення привілейованих користувачів. GPO:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Deny log on through Remote Desktop Services Administrator, NT AUTHORITY\Local Account

Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation

Remote host allows delegation of non-exportable credentials Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client

Configure server authentication for client Enabled. Authentication setting: Do not connect if authentication fails

Do not allow passwords to be saved Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections

Allow users to connect remotely by using Remote Desktop Services Enabled

Deny logoff of an administrator logged in to the console session Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection

Do not allow Clipboard redirection Enabled

Do not allow drive redirection Enabled

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\

Remote Desktop Session Host\Security

Always prompt for password upon connection Enabled

Do not allow local administrators to customize permissions Enabled

Require secure RPC communication Enabled

Require use of specific security layer for remote (RDP) connections Enabled

Require user authentication for remote connections by using Network Level Authentication Enabled

Set client connection encryption level Enabled, Security Layer: SSL

Encryption Level: High Level

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Allow log on through Remote Desktop Services Remote Desktop Users

Deny log on through Remote Desktop Services Administrators, NT AUTHORITY\Local Account

36. Заборонити неавторизований виклик віддаленого виклику процедур (RPC). GPO:

Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call

Restrict Unauthenticated RPC clients Enabled

RPC Runtime Unauthenticated Client Restriction to Apply: Authenticated

37. Заборонити неавторизоване використання спільних мережевих ресурсів та протоколу SMB. GPO:

Computer Configuration\Policies\Administrative Templates\MS Security Guide

Configure SMB v1 client driver Enabled

Configure MrxSmb10 driver: Disable driver (recommended)

Configure SMB v1 server Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

Microsoft network client: Digitally sign communications (always) Enabled

Microsoft network client: Digitally sign communications (if server agrees) Enabled

Microsoft network client: Send unencrypted password to third-party SMB servers Disabled

Microsoft network server: Amount of idle time required before suspending session 15 minutes

Microsoft network server: Digitally sign communications (always) Enabled

Microsoft network server: Digitally sign communications (if client agrees) Enabled

38. Заборонити використання Microsoft Store Apps. GPO:

Computer Configuration\Administrative Templates\Windows Components\ Store Turn off the Store application Enabled

39. Вимкнути Windows10 keylogger:

Start \ Settings \ Privacy \ Speech. Inking. & typing

Select Turn Off speech services and Typing suggestions