Державна служба спеціального зв'язку та захисту інформації України
Команда реагування на комп'ютерні надзвичайні події України CERT-UA

Рекомендації щодо підвищення рівня захищеності інформаційно-телекомунікаційних систем та інформаційних ресурсів державних органів і установ

1. Оновити програмне забезпечення серверного обладнання, пристроїв захисту та автоматизованих робочих місць (далі - АРМ) користувачів. В рамках зазначеного, особливу увагу приділити критичним оновленням та оновленням безпеки операційних систем (далі - ОС), оновленням веб-браузерів, програм для роботи з текстом та медіа контентом. Для реалізації оновлення ОС та програмного забезпечення виробництва компанії Microsoft, як приклад, встановити сервер WSUS та налаштувати АРМ та серверне обладнання на автоматичне оновлення.

З метою відслідковування випуску нових версій та оновлень програмних продуктів інших виробників, адміністраторам інформаційно-телекомунікаційних систем (далі - ІТС) забезпечити підписку на відповідні стрічки новин (RSS), поштові розсилки тощо.

2. Активувати використання стандартних міжмережевих екранів (брандмауерів) та/або встановити додаткове програмне забезпечення, яке реалізує зазначені функції.

3. У випадку використання в ІТС доменної архітектури, за допомогою групових політик та служби каталогів Active Directory забезпечити делегування необхідних повноважень та привілеїв визначеним групам користувачів. У випадку використання робочих груп, забезпечити створення облікових записів для користувачів з обмеженими привілеями, уникнувши ситуацій, коли кожен зі співробітників відомства є адміністратором на своєму АРМ.

4. Переглянути парольну політику з метою виявлення нестійких паролів, паролів, встановлених за замовчуванням або не встановлених взагалі. Розробити єдині вимоги щодо складності паролю, частоти та порядку його зміни, а також забезпечити контроль за їх виконанням. Уникнути випадків зберігання логінів та паролів у відкритому вигляді на робочих столах моніторів та інших місцях файлової системи ОС, а також на паперових носіях інформації біля моніторів, клавіатур та інших загальнодоступних місць. На програмному рівні заборонити зберігання логінів та паролів у веб-браузерах, утилітах для роботи з базами даних, або іншому клієнтського програмному забезпеченні (Total Commander, FTP-, SSH-клієнтах тощо).

5. Вжити необхідних заходів щодо регламентування порядку підключення до АРМ змінних носіїв інформації (вимкнути функцію автозапуску, забезпечити проведення автоматичної перевірки на наявність шкідливого програмного забезпечення тощо), відключити можливість підключення по нульовій сесії (в залежності від типу ОС, внести необхідні значення в реєстр), визначити

Ukraine
04119, Kyiv
Melnikova str., 83b
Tel. +380 44 281 88 01
Fax. +380 44 489 31 33

Україна
04119, Київ
Мельникова вул., 83б
Тел. +380 44 281 88 01
Факс. +380 44 489 31 33

Украина
04119, Киев
Мельникова ул., 83б
Тел. +380 44 281 88 01
Факс. +380 44 489 31 33

www.cert.gov.ua

порядок доступу до share-ресурсів, ліквідувавши можливість анонімного підключення та модифікації їх вмісту.

6. Ліквідувати можливість несанкціонованого встановлення користувачами стороннього програмного забезпечення, зобов'язавши останніх погоджувати зазначені заходи з адміністратором безпеки ІТС. Уникнути використання на АРМ співробітників сервісів та служб, які не є необхідними для виконання ними своїх службових обов'язків. На серверному обладнанні забезпечити відключення/фільтрацію служб/портів, які не використовуються.

7. При організації корпоративного електронного поштового обміну на поштовому сервері налаштувати використання захищених протоколів, таких як POP3S (IMAP4S), SMTPS, уникнувши тим самим передавання автентифікаційної інформації (логінів та паролів) у відкритому вигляді.

8. Під час здійснення віддаленого адміністрування активного мережевого, серверного обладнання та пристроїв захисту, використовувати захищені протоколи SSH, HTTPS, SCP, FTPS. Можливість доступу по незахищеним протоколам (TELNET, HTTP тощо) має бути відключена програмно. Крім того, можливість підключення до апаратного забезпечення з метою адміністрування повинна бути обмежена за допомогою списків контролю доступу (ACL) для визначеного кола осіб.

9. Для ліквідації можливості організації несанкціонованих підключень до ІТС, порти активного мережевого обладнання, які не використовуються, перевести в режим «administratively down» («disabled»).

За наявності такої можливості, здійснювати контроль підключень до ІТС за допомогою опції «port security» на комутаторах, забезпечивши фільтрацію по MAC-адресам.

Також, зазначене може бути досягнуто шляхом впровадження технології IEEE 802.1x або використанням спеціалізованих протоколів RADIUS, KERBEROS, TACACS+ та інших.

10. З метою ліквідації broadcast-штормів, а також для відокремлення інформаційних потоків, які містять персональні дані та іншу інформацію, доступ до якої має бути обмежено, АРМ співробітників підрозділів кадрового забезпечення, бухгалтерії та інших рекомендується розмістити в окремих мережевих сегментах шляхом створення фізично відокремлених мереж для вищезазначених підрозділів та/або за допомогою застосування технології віртуальних локальних обчислювальних мереж (VLAN).

11. З метою ліквідації можливості отримання несанкціонованого доступу до технологічних інформаційних потоків, які виникають під час здійснення віддаленого адміністрування, передбачити створення адміністративного VLAN або вжити заходів з фізичного відокремлення адміністративного мережевого сегменту (наприклад, використовувати IP KVM).

12. Здійснювати регулярний контроль над організацією несанкціонованих підключень елементів ІТС відомства (за допомогою модемів, Wi-Fi-маршрутизаторів тощо) до інших мереж передачі даних (в т.ч. Інтернет). У випадку необхідності використання бездротових мереж, забезпечити їх фізичне відокремлення від ЛОМ відомства; для автентифікації використовувати технологію WPA2 (стандарт IEEE 802.11i).

13. За допомогою антивірусного програмного забезпечення (АВПЗ) проводити сканування АРМ на предмет наявності шкідливого програмного забезпечення. Регулярно здійснювати оновлення АВПЗ (державним органам керуватися наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45 та вжити заходів щодо організації отримання оновлень з веб-сайту Центру антивірусного захисту інформації Держспецзв'язку).

14. Забезпечити ведення моніторингу працездатності активного мережевого, серверного обладнання, засобів захисту та каналів зв'язку. Як приклад, використовувати відповідне програмне забезпечення (Cacti, Nagios, Munin, MRTG, Zabbix) та можливості протоколу SNMP, попередньо змінивши встановленні за замовчуванням значення «community string».

15. Розробити регламент резервного копіювання критичних інформаційних ресурсів та конфігурацій апаратного забезпечення, а також передбачити порядок відновлення працездатності елементів ІТС на випадок збоїв.

16. З метою забезпечення можливості з'ясування об'єктивних обставин та причин на випадок порушення штатного режиму функціонування елементів ІТС або витоку інформації внаслідок несанкціонованих дій, забезпечити здійснення реєстрації та журналювання системних подій і подій безпеки (програмні або апаратні збої, доступ до баз даних, адміністративний доступ до обладнання та інше) та здійснювати їх регулярний аналіз.

17. Передбачити проведення занять, спрямованих на підвищення обізнаності співробітників відомства щодо безпечного користування сервісами електронної пошти, передачі файлів, перегляду інформаційних ресурсів, розміщених в мережі Інтернет, а також описати порядок дій користувачів у разі виявлення ознак порушення штатного режиму функціонування інформаційних систем чи елементів ІТС в цілому.

18. Вжити заходів з розробки необхідних інструкцій та положень, які б формалізували перелік заходів, спрямованих на забезпечення інформаційної безпеки в ІТС (політика інформаційної безпеки в ІТС, план захисту інформації, інструкція користувача АРМ тощо).

Звертаємо увагу на необхідність врахування вимог чинного законодавства у сфері захисту державних інформаційних ресурсів:

- Закон України «Про інформацію»;

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про персональні дані»;
- «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (затверджені постановою КМ України від 29.03.2006 № 373);
- НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;
- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;
- НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

У разі виявлення фактів несанкціонованих дій по відношенню до елементів ІТС державних органів чи державних інформаційних ресурсів, відповідальні особи вживають заходів щодо фіксації обставин і технічних деталей здійснення атаки та за допомогою електронної пошти (cert@cert.gov.ua) чи електронної форми на офіційному веб-сайті www.cert.gov.ua повідомляють фахівців CERT-UA стосовно комп'ютерного інциденту.

Ukraine
04119, Kyiv
Melnikova str., 83b
Tel. +380 44 281 88 01
Fax. +380 44 489 31 33

Україна
04119, Київ
Мельникова вул., 83б
Тел. +380 44 281 88 01
Факс. +380 44 489 31 33

Украина
04119, Киев
Мельникова ул., 83б
Тел. +380 44 281 88 01
Факс. +380 44 489 31 33