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 від несанкціонованих дій зі сторони мережі Інтернет

1. Оновити до актуальної версії операційні системи, системи керування контентом (CMS) та відповідні плагіни та інше програмне забезпечення (драйвери, додатки, засоби мультимедіа), а також забезпечити встановлення необхідних критичних оновлень та оновлень системи безпеки на серверному обладнанні.

2. За допомогою апаратних та/або програмних (pf, ipfw, iptables) міжмережевих екранів забезпечити фільтрацію вхідних інформаційних потоків за принципом «заборонено все, що не дозволено», а також обмежити доступність зі сторони мережі Інтернет всіх портів, окрім тих, які необхідні для функціонування WEB-серверу (80/tcp, 8080/tcp тощо).

3. Переглянути парольну політику та змінити нестійкі паролі, паролі, встановленні за замовчуванням, а також ліквідувати ситуації, коли паролі не використовуються взагалі.

4. Регулярно (раз на тиждень) здійснювати резервне копіювання WEB-сторінки та передбачити можливість відновлення її функціонування з резервної копії.

5. Забезпечити журналювання подій за допомогою відповідного програмного забезпечення (apache, nginx, IIS); зберігати журнальні файли з деталізацією по кожному з днів протягом місяця.

6. Обмежити доступ до адміністративних розділів WEB-сторінки (панелей керування) зі сторони мережі Інтернет переліком визначених IP-адрес; для виконання завдань віддаленого адміністрування використовувати захищені протоколи (ssh, scp, https), уникнувши використання таких протоколів, як http, ftp, telnet та інших; провести сканування на вразливості автоматизованих робочих місць адміністраторів ІТС.

7. Встановити мінімальні привілеї для користувачів мережі Інтернет при доступі до файлів та папок (директорій) WEB-серверу, обмеживши їх правом «тільки читання»; уникнути (наприклад, за допомогою можливостей httpd.conf або .htaccess) можливість перегляду лістингу директорій та файлів WEB-серверу зі сторони мережі Інтернет.

8. Ініціювати перевірку вихідних кодів WEB-сторінок на предмет наявності вразливостей, що виникають при недостатній та/або некоректній фільтрації (обробці) вхідних даних (атаки типу JS-, PHP-, SQL-ін'єкції, XSS та інші).

9. Для зменшення навантаження на систему керування базами даних WEB-серверу, реалізувати схему включення WEB-серверу за принципом «front-end - back-end».

10. Застосовувати системи виявлення/попередження вторгнень (IDS/IPS) та інші програмно-апаратні пристрої захисту.

11. З метою забезпечення доступності WEB-серверу на випадок здійснення розподіленої атаки на відмову в обслуговуванні (DDoS), узгодити з відповідальним оператором (провайдером) телекомунікацій порядок оперативного підвищення пропускної здатності каналів зв'язку.

12. З урахуванням вимог «Порядку координації діяльності координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, який зареєстровано в Міністерстві юстиції України 07.07.2008 за № 603/15294, розробити регламент своєчасного інформування CERT-UA щодо факту несанкціонованих дій.

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