ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ

Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку для підвищення рівня захисту інформаційних ресурсів та систем і для запобігання кіберінцидентам в установах, на підприємствах і в організаціях

За результатами усунення наслідків кібератак на ресурси об'єктів фінансового, транспортного, енергетичного секторів України Державна служба спеціального зв'язку та захисту інформації України рекомендує здійснити ряд організаційних заходів в установах, на підприємствах і в організаціях з метою запобігання кіберінцидентам і сприяння підвищенню рівня кіберзахисту електронних ресурсів та систем, а саме:

1. Провести аудит запроваджених заходів захисту та рівня інформаційної безпеки систем у цілому.

2. Провести роз'яснювальну роботу з працівниками, які користуються службовою електронною поштою, щодо правил та вимог безпеки, особливо в частині, що стосується вхідних листів (повідомлень).

3. Заборонити відкриття вкладень у підозрілих повідомленнях (листах від адресатів, щодо авторства яких виникають сумніви, наприклад: автор з невідомих причин змінив мову спілкування; тема листа є нетиповою для автора; спосіб, у який автор звертається до адресата, є нетиповим тощо; а також повідомленнях з нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів – архівів, виконуваних файлів тощо) та зобов'язати користувачів службової електронної пошти негайно повідомляти про такі листи адміністратора безпеки.

4. Зобов'язати користувачів службової електронної пошти провести її ревізію на предмет виявлення листів, що мають вкладення

«MoF critical IT needs_eng.xls», «Додаток №2.xls», заборонивши їх відкриття, та невідкладно повідомляти про наявність таких листів адміністратора безпеки.

5. Заборонити використання приватної електронної пошти для цілей службової діяльності.

6. Заборонити використання точок публічного доступу до Інтернет для входу до службової електронної пошти.

Адміністраторам безпеки рекомендовано:

1. Звести до мінімуму мережеву активність усіх пристроїв систем управління з Інтернет.

2. Ужити заходів до дотримання вимог із сегментування (виокремлення адміністративного VLAN, сегмента для серверів, окремих сегментів для бухгалтерії та кадрового підрозділу тощо), не допускати циркуляції технологічної інформації поза межами адміністративного сегмента мережі.

3. Для організації віддаленого доступу використовувати лише безпечні методи (наприклад, такі технологічні рішення, як VPN).

4. Для унеможливлення проведення атак типу Man-in-the-Middle з використанням техніки ARP-spoofing ужити заходів з налаштування статичних значень ARP-таблиць АРМ і серверного обладнання. Для цього здійснити прив'язку MAC-адрес АРМ до конкретного інтерфейсу комутатора, цим самим заборонивши підключення сторонніх пристроїв.

5. Передбачити моніторинг та фіксацію (журналювання) подій, які мають відношення до інформаційної безпеки (доступ до баз даних, адміністративний доступ до обладнання тощо).

6. Запровадити політику, що потребує використання лише надійних паролів.

Під надійними паролями слід розуміти такі, що:

– допускають використання не менше 8 символів;

- включають літери, цифри та спеціальні символи;
- не містять персональної інформації (дати народження своєї та своїх близьких, номерів телефонів, номерів та серій документів, що посвідчують особу, номерів власного автотранспорту, банківської картки, адреси реєстрації тощо);
- не використовуються в будь-яких інших аккаунтах.

7. Заборонити використання паролів, що були встановлені виробником обладнання «за вмовчанням», провести перевірку такого обладнання та в разі виявлення порушень привести його у відповідність до політики надійних паролів.

8. Провести рекомендоване виробником оновлення програмного забезпечення, щоб запобігти вже виявленим уразливостям.

9. Контролювати створення аккаунтів на рівні адміністраторів системи.

10. Здійснити зміну авторизаційних даних до критично важливих вузлів системи, попередньо перевіривши їх на наявність процесів, які можуть скомпрометувати дані.

11. Проводити постійний аналіз вхідного/вихідного Інтернет-трафіку.

12. Провести аналіз лог-файлів мережевого та серверного обладнання на наявність у них відомостей про аномальну активність (доступ до системи із систем, які перебувають поза адміністративним сегментом мережі; наявність нелегітимних авторизаційних даних).

13. Здійснити перевірку ПЕОМ адміністраторів мережі та критично важливих вузлів системи на наявність підозрілих процесів і програм (наприклад: системних служб, що запускаються не зі стандартного розташування; програм, що не мають цифрового підпису виробника, тощо).