RAK
SECURITY SOLUTIONS DISTRIBUTOR

Бизнес Парк „София", София 1766
тел.: 02 401 66 00, 0897 807 600, факс: 02 401 65 45
e-mail: office@rak.bg, http://www.rak.bg

ПРЕПОРЪКИ ЗА ИЗБЯГВАНЕ НА ПРОБЛЕМИ С КИБЕР СИГУРНОСТТА С УСТРОЙСТВА НА РАК ООД

Бюлетин
01/2017

Уважаеми клиенти,

Във връзка с избягване на проблеми със сигурността на устройства марка TVT и Dahua дистрибутирани от фирма РАК ООД.

Става въпрос за кибер DDoS атаки от неизвестен източник (за сега). При устройства на TVT след засягането им, започват да генерира сериозно количество трафик и като краен резултат блокира локалните мрежи на клиентите, което ги прави на практика неизползваеми.

Основен проблем при Dahua е промяната на мрежовите настройки на устройството (IP, Mask, Gateway) и последваща липса на дистанционна връзка с него, промяна в името на каналите, промяна на зададените потребители и пароли, HCVR не визуализират включените камери, респективно и не записват.

За решаване на проблема е задължително да се обнови фърмуеъра на устройството до последна версия от FTP сървъра на фирма РАК ООД:

ftp://92.247.81.210/FTP/Dahua/Firmware/HCVR_XVR/
ftp://92.247.81.210/FTP/Dahua/Firmware/NVR/

Задължително след префлашване на заразеното устройство привеждане до фабрични настройки (default settings).

Задължително префлашване и на новозакупеноте устройства с последни версии на FW с цел превенция.

Допълнителни мерки с цел превенция изразяваща се в следните стъпки:

1) задължителна промяна на фабричните пароли за всички потребители на устройствата. Препоръчителна дължина: минимум 8 символа съдържаща цифри, главни и малки букви както и специални символи;
2) задължителна промяна на фабричните портове (HTTP:80 и TCP/IP:37777)на машините;
3) задължително спиране на DMZ услугата (понеже отваря всички портове) и извеждане на 2-та порта (повече при нужда) през NAT-а на рутера (Port forward);
4) Използвайте сертификат за сигурност или криптирана връзка (HTTPS) за комуникация с вашите устройства;
5) Използвайте IP филтър за редуциране на IP адресите от който може да се достъват устройствата ви.

За допълнителни препоръки относно сигурността от тук:
ftp://92.247.81.210/FTP/Dahua/Manuals/temp/How%20to%20Create%20a%20More%20Secure%20Security%20System.pdf

Относно превенция и избягване на възможност за заразяване на устройства на марка TVT, трябва да се осъществи стандартно префлашване на фърмуеъра на устройството от тук:
ftp://92.247.81.210/FTP/CCTV/DVR/TVT/Firmware/Lastest%20version/telnet%20port/
Като първо сверявате модела си от тук:

ftp://92.247.81.210/FTP/CCTV/DVR/TVT/Firmware/Lastest%20version/telnet%20port/Attachment_FTP_Link_for_FW-20170412_1.xls
Инструкция за обновяване на FW от тук:
ftp://92.247.81.210/FTP/CCTV/DVR/TVT/Firmware/Lastest%20version/telnet%20port/Upgrade_FW_TVT.pdf

Ако устройството вече е заразено, не се достъпва, не стартира или има друг симптом моля, обърнете се към колегите от сервизния отдел на ф-ма РАК ООД.

За контакти сервизен отдел: +359 893 329 794, технически отдел: +359 893 329 793