Jak zvýšit bezpečnost zařízení DAHUA

Kybernetická bezpečnost není jen módním slovem, tento problém se týká všech zařízení, která jsou připojeny k síti „Internet“. Je důležité si uvědomit, že monitorovací zařízení (IPC, NVR, HDCVR, ...) nejsou imunní vůči kybernetickým útokům a jejich rozhraní pro konektivitu nenahrazují funkci Firewallu nebo jiných podobných zařízení.

Níže popsané doporučení Vám mohou pomoci těmto útokům předcházet a mohou Vám snížit bezpečnostní riziko, které je nejvyšší při ponechání zařízení s továrními hodnotami.

Obsah

1. Změna hesla za silnější

Pro někoho základní postup při zprovoznění zařízení, ale nejvíce úspěšných útoků je právě díky slabému heslu nebo ponechání výchozího hesla z výroby. Silné heslo lze považovat takové, které obsahuje číslice, speciální znaky a kombinaci velkých a malých písmen. Dále doporučujeme toto heslo po určitém období měnit. Zde je 10 nejčastěji používaných hesel:

123456	heslo	12345678	qwerty	12345
123456789	master	1234	1234567	admin

Toto jsou nejčastěji používaná hesla, která jsou nastavena jako první při pokusu prolomit Váš účet. Reálný seznam těchto hesel se počítá v řádu tisíců.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/change-user-name-or-password.html

2. Aktuální Firmware

Standardem u operačních systémů je mít nejnovější aktualizace, které obsahují nejnovější bezpečnostní „záplaty“ a opravy. To stejné doporučujeme i u zařízení Dahua. Vždy si zkontrolujte, jestli máte nejnovější FW pro dané zařízení. U každé verze FW je vždy „Build date“ ten značí datum vydání používaného FW. V případě, že FW je starší více než 18 měsíců kontaktujte naši technickou podporu společnosti TSS Group.

3. Změna výchozích TCP portů

Doporučujeme změnit výchozí port pro HTTP a TCP. To jsou dva nejčastěji používané porty pro vzdálenou komunikaci se zařízeními Dahua po sítí / na dálku. Tyto porty lze změnit v rozmezí 1025-65535. Použitím jiných než standardních portů snížíte riziko útoků. Útoky jsou často zautomatizované a předpokládají například u HTTP port 80.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/nvr-interface-setting-network.html#Connection

4. Povolení HTTPS a SSL

Nastavte si SSL certifikát a povolte HTTPS. Tímto nastavením bude veškerá Vaše komunikace šifrována a eliminujete možnost „odposlechnout“ vaši komunikaci mezi zařízením a Vámi.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/how-to-create-and-install-a-certificate.html

5. IP Filtr

Pro zvýšení bezpečnosti doporučujeme nastavit seznam povolených IP adres. Přístup ze zařízení, které mají IP adresu uvedenou v tomto seznamu, se mohou na zařízení připojit.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/nvr-interface-setting-network.html#IP_Filter

6. Změna hesla pro ONVIF

Na starších zařízení IPC se heslo pro ONVIF nezměnilo po změně hesla pro přístup do systému. Kontaktujte technickou podporu TSS Group a zkontrolujte, jestli v zařízení používáte nejnovější Firmware. Nebo nastavte heslo pro ONVIF manuálně.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/change-onvif-password-via-onvif-device-manager.html

7. Přesměrujte pouze potřebné porty

Doporučujeme přesměrovat na zařízení pouze porty pro HTTP a TCP. Nedoporučujeme povolovat rozsah portů anebo funkci DMZ směrované na „koncové“ zařízení Dahua. V případě, že máte kamery připojené do rekordéru, není potřeba na tyto kamery přesměrovávat jakoukoliv komunikaci/porty. Stačí přesměrovat pouze HTTP a TCP porty na rekordér.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/how-to-setup-remote-access-for-nvr.html

8. Auto-login do SmartPSS

Jestli používáte SmartPSS na zařízení, které může využívat více uživatelů ujistěte se, že není povolen Auto-login do SmartPSS. Tím zamezíte přístupu uživatelům, kteří si spustí aplikaci SmartPSS na zařízení a nemají udělený přístup. V aplikaci SmartPSS nedoporučujeme používat stejné uživatelské jméno a heslo jako je použito do zařízení Dahua.

9. Omezení uživatele pouze na funkce, které potřebují

Jestli zařízení Dahua využíváte pro více uživatelů současně, ujistěte se, že každý uživatel má pouze ty oprávnění, které skutečně potřebuje ke své činnosti.

10. UPNP

UPNP se snaží automaticky nastavovat potřebné porty na routeru nebo modemu. Za normálních okolností je dobrý pomocník a usnadňuje práci. Nicméně pokud Váš systém sám přesměruje porty a zařízení je ve výchozím stavu může toto nastavení zneužít útočník. Doporučujeme porty pro HTTP a TCP nastavit na routeru manuálně a tuto funkci ponechat vypnutou.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/upnp-function.html

11. SNMP

Jestli nevyužíváte SNMP doporučujeme tuto funkci zakázat. V případě, že tuto funkci potřebujete, doporučujeme ji nechat povolenou pouze po dobu potřebnou pro testování nebo sledování.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/snmp.html

12. Multicast

Multicast se používá ke sdílení video streamů mezi dvěma rekordéry. V současné době nejsou známy žádné bezpečnostní rizika týkající se multicastu. V případě, že tuto službu nevyužíváte, vypnutím této služby můžete zvýšit zabezpečení zařízení.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/nvr-interface-setting-network.html#Multicast

13. Kontrola LOGů

Jestli máte podezření, že jste se staly obětí útoku anebo se někdo neoprávněný snažil do Vašeho zařízení přihlásit, zkontrolujte logy zařízení. Logy Vám mohou ukázat, z jaké IP adresy se útočník pokoušel přihlásit a co bylo nebo nebylo povoleno.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/nvr-interface-info-log.html

14. Fyzické zabezpečení zařízení

Pokud to situace dovoluje, doporučujeme zařízení umístit do uzamykatelné místnosti. Nejlépe tento prostor posílit docházkovým a bezpečnostním systémem.

15. Připojení kamer do PoE portů

Kamery připojené pomocí PoE portů v zadní části rekordérů (v případě, že rekordér těmito porty disponuje) jsou kamery isolovány od jakékoliv venkovní komunikace. Na kamery se nelze zvenčí přihlásit.

Návod s videem jak postupovat naleznete zde (v EN):

http://www.dahuasecurity.com/how-to-connect-camera-to-nvr.html

16. Sítě bezpečnostních technologií

Je-li počítačová síť rozdělena do několika segmentů a obsahuje nějakou hierarchii (například VLANy), doporučujeme v této síti vyčlenit pro bezpečnostní prvky a zařízení speciální segment a do něj povolit přístup pouze vybraným zařízením/uživatelům. Tím zamezíte přístupu k zařízení návštěvám a jiným nežádoucím uživatelům.

17. Účet 888888

Účet 888888 je možné použít pouze lokálně na zařízení (pomocí obrazovky a myši připojené k rekordéru). Nelze se jím přihlásit vzdáleně (webové rozhraní, SmartPSS, atd.). Nelze u něj ani snížit oprávnění. Tento účet je vždy nadřazen všem účtům v systému. Proto je doporučováno změnit heslo pro tento účet a omezit k zařízení fyzický přístup (viz bod: 14).