Twiin Portaal

Aanbevelingen voor een veilige keten

Vertrouwen is een cruciaal element voor het functioneren van netwerken. Zo ook voor het landelijke Twiin Portaal netwerk. VZVZ heeft een periodieke risico-inventarisatie en evaluatie bij een deelnemer uitgevoerd. De centrale infrastructuur is veilig. Het deel van de keten waar VZVZ geen zicht op heeft zijn de begin- en eindpunten; deze bevinden zich op het interne netwerk van de gebruikers van het Twiin Portaal. Gezien de keten zo sterk is als de zwakste schakel, is het dringende advies om periodiek te controleren welke risico's en kwetsbaarheden bij u als gebruiker kunnen voorkomen om passende maatregelen te nemen. Dit document komt met praktische aanbevelingen en is bedoeld voor de beheerders van de Twiin Gateway, beeldimportserver en/of PACS-servers en koppelingen bij de deelnemer.

Aanbevelingen informatiebeveiliging Twiin Portaal

Naast de algemene aanbeveling om periodiek de risico's en beveiligingsmaatregelen te evalueren en waar nodig bij te stellen, heeft VZVZ de volgende specifieke aanbevelingen:

- ☐ Harden servers, met name de Twiin Gateway, beeldimportserver en PACS;
- ☐ Verstuur de DICOM data over een versleutelde verbinding;
- ☐ Beperk lokale beheerrechten;
- ☐ Hanteer voor externe toegang betere 2FA-methodieken;
- ☐ Stel beheeraccounts op naam;
- ☐ Beperk de toegang tot de beheerservices.

Hieronder worden deze specifieke aanbevelingen verder toegelicht.

Harden servers

Verzeker u dat de beheerdiensten niet worden aangeboden aan een groter publiek dan noodzakelijk. Scherm de services af, zodat ze alleen toegankelijk zijn vanaf de systemen die een legitieme reden hebben om de services te gebruiken. Maak services voor beheer alleen beschikbaar vanaf een hiervoor bestemd beheernetwerk. Maak daarnaast duidelijke afspraken met de leverancier met betrekking tot server hardening. Meer informatie kunt u vinden bij het Center for Internet Security (CIS). Zij publiceren benchmarks ten behoeve van hardening van gangbare softwareproducten.

Verstuur de DICOM data over een versleutelde verbinding

Een aanvaller die een MitM-positie[1] weet te verkrijgen in het netwerksegment van de Twiin Gateway, beeldimportserver of PACS-servers, kan de DICOM-data onderscheppen en uitlezen, bijvoorbeeld door een ARP-spoofing aanval uit te voeren. Verstuur tussen deze servers de DICOM-data over een versleutelde verbinding. Voor meer informatie: het NCSC publiceert onder andere richtlijnen voor transportbeveiliging.

Beperk lokale beheerrechten

Engineers van leveranciers of aanvallers die een supply-chain aanval over een leverancier uitvoeren, hebben lokale beheerrechten op servers. Op deze zelfde servers loggen geregeld ook beheerders van de zorginstelling in. Via deze lokale beheerrechten kan een aanvaller de accounts van de beheerders van de zorginstelling compromitteren en daarmee verdere aanvallen op het netwerk uitvoeren. Verleen alleen gedurende afgesproken tijden lokale beheerrechten aan leveranciers, wanneer deze daadwerkelijk nodig zijn voor beheerwerkzaamheden.

Hanteer voor externe toegang betere 2FA-methoden

Vermijd e-mail en SMS als kanaal om OTP codes te sturen. Aanvallers richten zich eerst op e-mail en SMS-kanalen, omdat deze kanalen relatief makkelijk te compromitteren zijn. Biedt andere vormen van 2FA aan, bijvoorbeeld via een Authenticator dat OTP codes genereert of door middel van hardwaretokens gegenereerd op basis van de U2F standaard. Voor meer informatie: zie de factsheet van NCSC.

Stel beheeraccounts op naam

Verzeker u dat gebruik wordt gemaakt van persoonsgebonden accounts voor de beheerders; van uw eigen organisaties als bij uw leveranciers. Wijzigingen dienen door middel van logging herleidbaar te zijn tot specifieke

[1] Man-in-the-middle

gebruikers. Geef precies voldoende (en niet meer) privileges aan de verschillende beheerders om hun werkzaamheden uit te kunnen voeren. Maak gebruik van persoonsgebonden accounts voor het beheer van de systemen.

Beperk de toegang tot de beheerservers

Als er geen gebruik wordt gemaakt van een gescheiden beheernetwerk, zijn alle beheerservices van de Twiin Gateway, beeldimportserver en PACS toegankelijk vanaf het gebruikersnetwerk en kunnen zo worden aangevallen. Richt een afgeschermd beheernetwerk in. Zorg ervoor dat de beheerservices op de servers alleen op de interfaces op dit beheernetwerk te benaderen zijn. Pas daarnaast firewall-regels toe om ervoor te zorgen dat deze services alleen toegankelijk zijn vanaf de systemen vanwaar er daadwerkelijk beheer plaatsvindt. Of maak gebruik van zogenaamde stepping stone systemen en zorg dat uitsluitend vanaf deze speciaal gehardende systemen beheer uit wordt gevoerd. Beheertooling staat alleen op deze systemen en niet op de persoonlijke werkplek van de beheerder.

Gebruik HTTPS certificaten

Bij de Twiin Gateway wordt standaard een webapplicatie meegeleverd, waarmee het ontvangen en verzenden van onderzoeken kan worden gedaan. De toegang tot deze applicatie dient uitsluitend via HTTPS plaats te vinden, zodat de verbinding tussen de eindgebruikers en de webapplicatie beveiligd is. Dit geldt ook als de webapplicatie binnen het interne netwerk van de deelnemer is geplaatst. Als een deelnemer dit nog niet heeft geactiveerd is, het verzoek om contact op te nemen met support@alphatronmedical.com.

Meewerken aan jaarlijkse updates en upgrades

Alphatron voert jaarlijks updates en upgrades van de software uit. Dit gebeurt om ervoor te zorgen dat de meest recente security updates geïnstalleerd zijn bij alle deelnemers in het netwerk. Hier is ook inzet van de deelnemers zelf vereist. Dit vraagt capaciteit, maar levert uiteindelijk een veilige en up-to-date keten op. Verzoek om hier dus capaciteit voor in te calculeren.

VZVZ adviseert om bovenstaande aanbevelingen met de verantwoordelijke beheerders en betrokken leveranciers te bespreken.

Tim Smits

Productverantwoordelijke Twiin Portaal

E-mail: tim.smits@vzvz.nl

Versie: 18 augustus 2022