Hoe beschermt PAM organisaties in de gezondheidszorg?

13 september 2022

Cybercriminelen azen op de financiële en gezondheidsgegevens van zorgorganisaties. Ze proberen bovendien zorgsystemen te blokkeren met ransomware of door gigantische verkeersvolumes (DDoS) te genereren. IT-securityteams moeten zich voortdurend bezighouden met deze problemen. Wet- en regelgeving, zoals de AVG en NEN7510, vereist dat, maar ook verzekeraars, toezichthouders en patiënten eisen de hoogste beveiligingsstandaarden.

Zorg staat voor unieke uitdagingen

De paradox van gedeelde gezondheidsinformatie is dat deze tegelijkertijd patiënten veiliger maakt en hen in gevaar brengt. Technologische innovatie brengt de kwaliteit van de gezondheidszorg op een hoog niveau. Het maakt zorgorganisaties echter ook aantrekkelijk voor cybercriminelen omdat elektronische patiëntendossiers een schat aan persoonlijke, medische en financiële informatie bevatten. Het EPD is voor een hacker een one-stop-shop.

Bovendien raadplegen de meeste mensen raadplegen weleens een of meer zorgverleners. Hierdoor is de informatie van bijna iedereen in een of andere vorm beschikbaar. Doordat elektronische medische dossiers onderling verbonden zijn, hebben hackers toegang tot patiëntgegevens die al jaren worden verzameld.

Zodra een hacker toegang heeft tot een netwerk, kan hij dit blokkeren met ransomware of ontregelen door DDoS-aanvallen, aldus zorgbeveiliger Z-Cert. Voor zorgorganisaties is dit

extra gevaarlijk omdat er, anders dan in het bedrijfsleven, mensenlevens op het spel staan. De beveiliging van medische gegevens en apparaten brengt daarom voor zorgorganisaties veel unieke uitdagingen met zich mee.

In deze sector weet men als geen ander: voorkomen is beter dan genezen. Kwetsbaarheden in apparaten en applicaties zetten de deur open voor cybercriminelen. Het is daarom belangrijk om altijd de meest recente updates te installeren. Ook de configuratie-instellingen dienen bijgewerkt te worden om hackers buiten de deur te houden. En als het toch eens mis mocht gaan moet een plan van aanpak zijn voor het herstel. Die taken neemt PAM voor zijn rekening.

Belang van PAM-oplossing

Allereerst is het van belang de toegangsrechten van alle gebruikers te beschermen. Dat begint met goed beheer: wie heeft er toegang tot welke apparaten, applicaties en gegevens en wat mag deze gebruiker daarmee doen? IT-beheerders wijzen deze rechten toe en regelen de permissies. Stel nu dat het mogelijk is om account van de IT-beheerder over te nemen. Dan heeft een cybercrimineel meteen de controle over alle gebruikersaccounts, de systeem configuraties en het netwerkverkeer. Daarom vragen de accounts van zogenoemde geprivilegieerde gebruikers om aanvullende beveiliging. Naast de algemene IT-beheerders zijn dit onder meer systeemmedewerkers, netwerkspecialisten, DevOps-specialisten en bestuurders.

Een PAM-oplossing is een platform waarin strategieën en hulpmiddelen samenkomen om geprivilegieerde toegang en permissies voor systemen, processen, accounts en gebruikers te beheren. Het zorgt ervoor dat gebruikers alleen de toegang hebben die nodig is om hun taken uit te voeren. In de praktijk maakt voorkomt en corrigeert PAM de schade als gevolg van onzorgvuldigheid van werknemers en aanvallen door cybercriminelen.

Hoe werkt het?

Binnen een PAM-platform worden de toegangsrechten en -gegevens van geprivilegieerde accounts in een veilige omgeving of ‘kluis’ gestopt. Dit voorkomt dat deze worden gestolen of dat er op een andere manier misbruik van wordt gemaakt.

Geprivilegieerde gebruikers krijgen vervolgens via het PAM-systeem (geautomatiseerde) toegang tot de rechten en vervolgens tot de systemen en omgevingen. De gebruikers worden hierbij geïdentificeerd en geauthentiseerd en vervolgens worden al hun toegangsactiviteiten gelogd en gemonitord voor eventueel verdacht en afwijkend gedrag. De rapportage is vervolgens beschikbaar voor audits van toezichthouders, verzekeraars en het bestuur.

Voordelen van PAM

Het gebruik van PAM levert zorgorganisaties een aantal positieve resultaten op. PAM vermindert de risico’s die gepaard gaan met externe aanvallen en interne onachtzaamheid. PAM beschermt IT-systemen ook bij het werken op afstand, wat voor veel professionals realiteit is geworden tijdens de coronapandemie.

Zoals gezegd zijn de geprivilegieerde toegangsrechten en -gegevens opgeslagen in een digitale kluis op een externe locatie. Zorgorganisaties hebben bovendien altijd alle IT-middelen in

kaart. Dit maakt het makkelijker om na een incident het recoveryproces te beginnen, met aanzienlijk minder downtime. Men sluit eenvoudig nieuwe servers aan en voorziet deze direct van de oude toegangsrechten en configuratie-instellingen.

Tot slot draagt PAM bij aan het naleven van wet- en regelgeving, de eisen van toezichthouders en verzekeraars, en het beveiligingsbeleid van een zorgorganisatie. Het maakt aantoonbaar dat de organisatie de vertrouwelijkheid van de gegevens bewaakt. Zo draagt PAM bij aan de primaire taak van zorgorganisaties: de zorg voor patiënten, in de breedste zin van het woord.