Hoe beveiligt u uw gegevens in een productieomgeving?

01 maart 2022, 01:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

Sirris lanceerde onlangs haar cyberbeveiligingsdienst voor de maakindustrie. Naarmate we bedrijven benaderen via een gratis intake of een individuele coaching, krijgen we steeds meer vragen over hoe we gegevens kunnen beschermen in een productieomgeving waar machines en activiteiten steeds meer met elkaar verbonden zijn. Gegevens volledig afschermen tegen cyberaanvallen is een complexe aangelegenheid, maar enkele goede beveiligingspraktijken kunnen het probleem alvast grotendeels verhelpen.

Er bestaat geen pasklare oplossing. De keuze van oplossingen voor de gegevensbescherming hangt in grote mate af van de systeemarchitectuur, de mogelijkheden van de machine en de gebruikte protocollen. Toch kan de implementatie van een aantal algemene veiligheidsregels het risico op gegevensinbreuk helpen verminderen.

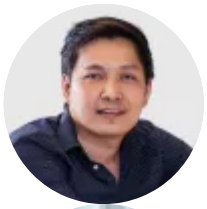
- De eerste belangrijke strategie die moet worden overwogen, is de **invoering van gegevenstoegangscontrole**. Pas het beginsel van de 'minimale bevoegdheid' toe, waarbij de gebruiker een minimum aan rechten krijgt toegewezen om zijn rol te vervullen. Gegevens die niet voor gebruikers bestemd zijn, mogen niet voor hen toegankelijk zijn. Dit kan onnodige toegang tot en gebruik van gegevens helpen voorkomen. Waar mogelijk moet een standaardprotocol voor toegangscontrole worden gehanteerd. Wanneer verouderde machines in gebruik zijn (waarbij alleen de traditionele combinatie van gebruikersnaam & wachtwoord mogelijk is) en geen geavanceerde toegangscontroletechnologie, zoals multifactor authenticatie, voorhanden is, is een goed wachtwoordbeheer noodzakelijk (bijv. beleid voor wachtwoorden en de vernieuwing ervan, ...). Vermijd één wachtwoord voor iedereen (bijv. één wachtwoord voor meerdere machines). De wachtwoorden moeten veilig worden bewaard. Gebruik een wachtwoordmanager als u meerdere wachtwoorden voor verschillende accounts of machines moet beheren. Er bestaan talrijke softwareprogramma’s voor wachtwoordbeheer, zowel open source als proprietary (bijv. KeePass, Bitwarden, ...). De gegevens moeten ook worden geclassificeerd volgens hun vertrouwelijkheidsniveau: hoe hoger de vertrouwelijkheid, hoe sterker de beveiliging moet zijn. Bij het bepalen van het toegangscontrolebeleid voor die gegevens wordt de rol van de gebruiker in een organisatie (bedrijf) gebruikt als voorwaarde voor het verlenen van toegang. De gegevens moeten bijvoorbeeld in verschillende categorieën worden opgedeeld, zoals financiële gegevens, personeelsgegevens, operationele gegevens (van machines en lokale communicatie) en intellectuele-eigendomsgegevens (IP).

- Een tweede strategie bestaat erin naar de **bescherming van inactieve gegevens** te kijken. In een productieomgeving produceren de machines doorgaans grote datahoeveelheden die in een datahistoriek worden bewaard. Deze gegevens moeten te allen tijde worden beveiligd en tegelijk toegankelijk worden gemaakt voor analyse. Er bestaan verschillende oplossingen om datahistorieken te beschermen; alles hangt ervan af of de opslag lokaal dan wel in de cloud is. De algemene regel is echter dat belangrijke of geheime gegevens cryptografisch moeten worden beschermd alvorens ze worden opgeslagen. Dit voegt een extra beschermingslaag toe aan de hierboven beschreven toegangscontrole. De op te slagen gegevens moeten vóór de opslag ook worden gescand, om te garanderen dat ze vrij zijn van virussen of malware. Er moeten meerdere kopieën van gegevens veilig worden bewaard op verschillende plaatsen om de risico's te beperken mochten gegevens worden beschadigd of gehackt (bijv. ransomware). Bij het maken van back-ups van gegevens moet een 3-2-1 back-upstrategie worden gehanteerd (3 kopieën van de gegevens (productiegegevens en 2 back-upkopieën) op twee verschillende media (schijf en tape) met één kopie off-site voor noodherstel.

- Een derde strategie bestaat erin te kijken naar **de veiligheid van de gegevens tijdens hun overdracht**. Dit behelst het veilig uitwisselen en delen van gegevens, lokaal of tussen locaties via een openbaar netwerk (bijv. het internet) of met een derde systeem (bv. toeleveringsketen of onderaannemer). Ook gegevens die lokaal worden uitgewisseld, moeten worden beschermd met behulp van een veilig/versleuteld communicatiekanaal (bijv. TLS of DTLS, ...) wanneer ze intern van de ene plek naar de andere worden verplaatst (bv. tussen netwerken). Als gegevens via een openbaar netwerk moeten worden verstuurd, is het aangeraden gebruik te maken van een VPN of een zero-trust-technologie, om een veilige tunnel tot stand te brengen voor het versturen of uitwisselen van gegevens.

- Met geavanceerde en gesofisticeerde hackingtools vinden aanvallers altijd wel een manier om in het netwerk/systeem binnen te dringen, hoe sterk de beveiliging ook is. Aanvallers kunnen buiten ons weten om toegang krijgen tot gegevens. Een **tool om de toegang tot de gegevens te monitoren** is dan ook een must. Met een dergelijke tool kan men de toegang van gebruikers tot gegevens controleren en tijdig waarschuwen wanneer een anomalie wordt gedetecteerd. Commerciële tools zoals Microsoft 365 en OneDrive bieden een auditlogboek dat kan dienen om de toegang tot en het delen van gegevens op het platform te controleren/op te volgen.

Auteurs



Annanda Rath



Christophe Michiels



Tatiana Galibus