Persbericht

Genetec adviseert door groei AI-cyberrisico's strengere authenticatiecontroles voor fysieke beveiligingssystemen

Ter gelegenheid van World Password Day waarschuwt Genetec dat het wijzigen van wachtwoorden alleen, niet langer voldoende is om fysieke security systemen te beschermen

Amsterdam, 6 mei 2026 —Genetec Inc. ("Genetec"), wereldwijd marktleider op het gebied van software voor fysieke beveiliging, adviseert om het beheer van toegangsrechten binnen connected fysieke beveiligingssystemen te verbeteren, nu met AI de cyberdreigingen steeds omvangrijker en geavanceerder worden.

Tools op basis van AI versnellen aanvallen op inloggegevens doordat ze de snelheid, schaal en nauwkeurigheid van attacks vergroten. Organisaties die werken met connected camera's, toegangscontrolesystemen, servers en clouddiensten, kunnen met zwakke of slecht beheerde inloggegevens risicovolle situaties creëren en criminelen toegang tot hun systemen geven. Dit geldt ook voor wachtwoorden waarmee je rechtstreeks verbinding maakt met beveiligingsapparatuur. Deze worden vaak over het hoofd gezien, maar kunnen een directe ingang bieden tot systemen, wanneer ze niet goed beheerd worden. Het is onvoldoende om alleen te vertrouwen op het regelmatig wijzigen van wachtwoorden of basismaatregelen voor cybersecurity.

"AI verandert de snelheid en omvang van cyberrisico's", zegt Mathieu Chevalier, Principal Security Architect bij Genetec Inc. "Hackers kunnen nog sneller handelen en gebruiken AI om zich voor te doen als andere personen, maken social-engineering aanvallen op maat, sporen kwetsbaarheden op grote schaal op en omzeilen detectie. Als reactie hierop moeten organisaties de toegang en identiteit binnen hun systemen actief beheren, in plaats van eenmalig security controles in te stellen en er maar op te vertrouwen dat deze effectief blijven."

Veel organisaties die een fysiek security systemen hebben, kregen al te maken met deze risico's. Uit recent onderzoek van Genetec, waaraan meer dan 7,300 fysieke security professionals meewerkten, blijkt dat 59 % te maken had met een toename in phishing en smishing aanvallen. 41% meldde een toename van het totale aantal fysieke of cyberincidenten en 43,5 % ziet social engineering als een van de belangrijkste aanvalsmogelijkheden.

Genetec adviseert organisaties verder te gaan dan geïsoleerde controles op inloggegevens, en een 'governance first'-benadering te hanteren voor identity management in fysieke beveiligingsomgevingen, met inbegrip van:

1. **Versterken van controle van identity en credentials**

Organisaties moeten standaard en gedeelde inloggegevens afschaffen, strenge authenticatie zoals passkeys toepassen en multi-factor authenticatie (MFA) invoeren om veelvoorkomende ingangen voor aanvallen te beperken. Dit geldt ook voor beveiligingsapparatuur: waar mogelijk moeten statische wachtwoorden worden vervangen door authenticatie op basis van certificaten, en moet worden gezorgd voor gecentraliseerd beheer en het regelmatig vervangen van credentials.

2. **Meer afstemming tussen IT en fysieke security teams**

Door betere afstemming tussen IT- en fysieke beveiligingsteams, kunnen consistente security standaarden toegepast worden, ontstaat er beter inzicht in toegangsrisico's en kan de respons op incidenten beter worden gecoördineerd. Naarmate fysieke security systemen steeds meer worden geïntegreerd in bedrijfsnetwerken, kan de afstemming tussen deze afdelingen helpen zwakke plekken op te sporen en effectiever te reageren op aanvallen waarbij misbruik wordt gemaakt van inloggegevens.

3. **Governance-first management**

Organisaties moeten hun fysieke security-infrastructuur met dezelfde zorgvuldigheid managen als andere bedrijfskritische systemen. Hierbij kan gedacht worden aan regelmatige reviews van toegang, gecontroleerde updates en partnerships met betrouwbare technologiepartners die zorgen voor veiligheid, transparantie en operationele veerkracht op de lange termijn.

Meer informatie is te lezen is ook te lezen in dit e-book van Genetec.

einde persbericht

Over Genetec

Genetec Inc. is een wereldwijd technologiebedrijf dat al meer dan 25 jaar de fysieke beveiligingsindustrie transformeert. Het portfolio van oplossingen van het bedrijf stelt bedrijven, overheden en communities wereldwijd in staat om mensen en bezittingen te beveiligen terwijl de operationele efficiëntie wordt verbeterd en de privacy van het individu wordt gerespecteerd. Genetec levert 's werelds toonaangevende producten voor videomanagement, toegangscontrole en ALPR, allemaal gebouwd op een open architectuur en ontworpen met cyberbeveiliging als uitgangspunt. Het portfolio van het bedrijf omvat ook oplossingen voor inbraakdetectie, intercom en digitaal bewijsmateriaalbeheer.

Het hoofdkantoor is gevestigd in Montreal, Canada. Genetec bedient zijn meer dan 42.500 klanten via een uitgebreid netwerk van geaccrediteerde channelpartners en consultants in meer dan 159 landen. Ga voor meer informatie over Genetec naar: www.genetec.com©

Perscontact:
Hilde Kok
In de Schijnwerpers
hilde@indeschijnwerpers.eu
Tel: +31(0)6 296 22 599