BEVEILIGING EN PRIVACY

Hoe veilig is uw Ajax-alarmsysteem?

Een overzicht van de beveiligingsmaatregelen in het Ajax-alarmsysteem dat Brepoels Security installeert, en van de afspraken over wie toegang heeft tot uw systeem.

Kort samengevat

- De draadloze communicatie tussen de detectoren en de centrale is versleuteld en elk toestel wordt bij elk contact gecontroleerd.
- De centrale communiceert via een versleutelde verbinding met Ajax Cloud en kan meerdere verbindingen tegelijk gebruiken.
- Storing van het radiosignaal (jamming) en sabotage worden gedetecteerd en gemeld.
- U beheert zelf wie het systeem mag bedienen en wie toegang heeft tot de instellingen.
- **Een installateur heeft enkel toegang tot de instellingen met de rechten die u hem geeft.**

1. Versleutelde draadloze communicatie

De detectoren, sirenes en bedieningstoestellen communiceren met de centrale (hub) via Jeweller, het eigen radioprotocol van Ajax:

- De gegevens worden versleuteld met een blokcijfer. Voor elke sessie tussen een toestel en de centrale wordt een nieuwe sleutel aangemaakt.
- Bij elk contact wordt het toestel geauthenticeerd. De centrale negeert signalen van toestellen die deze controle niet doorstaan. Zo kunnen toestellen en signalen niet nagebootst worden, bijvoorbeeld met een vervalste afstandsbediening.
- Een melding wordt herhaald tot de centrale bevestigt dat ze ontvangen is.
- De toestellen melden zich op een vast interval (instelbaar van 12 tot 300 seconden) bij de centrale, met hun batterijniveau, temperatuur en signaalsterkte. Valt een toestel weg, dan stuurt de centrale een melding.

2. Verbinding met Ajax Cloud en de meldkamer

- De centrale wisselt gegevens uit met de Ajax Cloud-server via een eigen, versleuteld communicatieprotocol. De AES-128-versleuteling van die verbinding is gevalideerd door NIST, het Amerikaanse National Institute of Standards and Technology. Authenticatie beschermt de server tegen nagebootste centrales.
- Ajax Cloud draait volgens Ajax in meerdere datacenters van Amazon Web Services.
- De server controleert regelmatig of de centrale nog verbonden is. Met de kortste instellingen worden gebruikers en de beveiligingsfirma ongeveer 60 seconden na het verbreken van de verbinding verwittigd.
- Is het systeem aangesloten op een meldkamer, dan kan het alarm rechtstreeks naar de meldkamer gestuurd worden, zonder via Ajax Cloud te passeren.

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · btw BE 1021.926.276
Vergunde onderneming FOD Binnenlandse Zaken voor alarm- en camerasystemen nr. 1021.926.276

3. Bescherming tegen storing en sabotage

- De centrale en de toestellen meten voortdurend de ruis op de radiofrequenties. Bij storing (jamming) worden de gebruikers en de beveiligingsfirma verwittigd en schakelt de centrale over naar een minder gestoorde frequentie.
- Afhankelijk van het model gebruikt de centrale meerdere verbindingen: ethernet, één of twee simkaarten en bij sommige modellen wifi. Valt er één weg, dan werkt de centrale verder via de andere.
- Vallen alle verbindingen weg, dan registreert de centrale de alarmen, stuurt ze de sirenes aan en verstuurt ze de opgeslagen meldingen zodra de verbinding hersteld is.
- De centrale heeft een sabotagecontact: wordt ze van de montageplaat gehaald, dan volgt er meteen een melding, ook als het systeem uitgeschakeld is.
- Bij het uitvallen van de netspanning neemt een noodbatterij het over. Hoe lang die volstaat, hangt af van het model en de configuratie.

4. Software van de centrale

- De centrale werkt met OS Malevich, een realtime besturingssysteem dat Ajax zelf ontwikkelt. Volgens Ajax is het beschermd tegen virussen en cyberaanvallen.
- Updates gebeuren automatisch via het internet, enkel wanneer het systeem uitgeschakeld is. Het updatebestand is versleuteld; volgens Ajax kent zelfs de server de sleutels niet.

5. U beslist wie toegang heeft

De beheerder (admin) van het systeem bepaalt wie het systeem mag bedienen en wie de instellingen mag wijzigen.

- Ajax maakt onderscheid tussen beheerders, gewone gebruikers (in- en uitschakelen, alarmen ontvangen) en PRO-accounts voor installateurs en beveiligingsfirma's.
- Een installateur heeft enkel toegang tot de instellingen als de beheerder dat toestaat: permanent of tijdelijk, voor 1, 2, 4 of 8 uur. Na die tijd worden de rechten automatisch ingetrokken.
- Foto's die detectoren met camera maken (bv. ter verificatie van een alarm) vallen onder de privacy-instellingen. Die worden beheerd door de beheerder; een installateur kan ze niet wijzigen.
- Ajax raadt af om volledige beheerdersrechten aan derden te geven, ook niet tijdelijk. Ajax kan geen toegang herstellen die verloren is gegaan door nalatigheid.
- De Ajax-app ondersteunt tweestapsverificatie (2FA).

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · btw BE 1021.926.276
Vergunde onderneming FOD Binnenlandse Zaken voor alarm- en camerasystemen nr. 1021.926.276

6. Normen en certificaten

NORM / CERTIFICAAT	WAT HET BETEKENT
EN 50131 (Grade 2)	Europese norm voor inbraakalarmsystemen. Volgens Ajax zijn alle inbraakdetectieproducten van de Baseline- en Superior-productlijnen gecertificeerd volgens Grade 2.
EN 50131 (Grade 3)	Hoger beveiligingsniveau, onder meer voor banken en juweliers. Een reeks Ajax Superior-toestellen, waaronder de Superior Hub Hybrid, is hiervoor gecertificeerd.
NIST-validatie AES-128	Validatie van de versleuteling tussen de Ajax-centrale en Ajax Cloud.
ETSI EN 303 645	Europese cyberbeveiligingsnorm voor IoT-toestellen. De Ajax Superior Hub Hybrid (4G) werd hiervoor gecertificeerd na testen door het labo Kiwa.
EN 18031	Europese cyberbeveiligingsnormen voor radioapparatuur. Volgens Ajax voldoet alle internetverbonden Ajax-radioapparatuur op de EU-markt hieraan.

Welke graad uw installatie haalt, hangt af van de geplaatste toestellen en de configuratie. Welke certificaten voor welk toestel gelden, staat op ajax.systems/standards.

7. Rol van Brepoels Security

Brepoels Security installeert en configureert uw systeem volgens de richtlijnen van de fabrikant. Na de oplevering ligt het beheer van de gebruikers en hun rechten bij u.

> **Toegang enkel met uw toestemming**
> Hebben wij voor onderhoud of een storing toegang tot de instellingen nodig, dan gebeurt dat met de rechten die u ons geeft. U kunt die toegang tijdelijk geven en op elk moment intrekken.

8. Uw verantwoordelijkheid als gebruiker

De technische beveiliging is maar zo sterk als het beheer van de toegang. De gebruiker is verantwoordelijk voor de wachtwoorden, codes en rechten die hij zelf beheert en toekent. Wij raden aan:

- Kies een sterk, uniek wachtwoord voor uw Ajax-account en schakel tweestapsverificatie in.
- Deel uw wachtwoord en de codes van het bedieningspaneel met niemand en kies codes die niet makkelijk te raden zijn.
- Geef gebruikers enkel de rechten die ze echt nodig hebben en verwijder gebruikers die geen toegang meer mogen hebben.
- Verwijder een verloren badge, tag of afstandsbediening meteen uit het systeem.
- Behoud zelf altijd de beheerdersrechten van uw systeem.
- Beveilig de smartphones en computers waarop de app geïnstalleerd is met een code of biometrie.

Brepoels Security is niet verantwoordelijk voor toegang tot het systeem die het gevolg is van gedeelde of zwakke wachtwoorden of codes, of van rechten die de gebruiker zelf aan anderen heeft toegekend.

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · btw BE 1021.926.276
Vergunde onderneming FOD Binnenlandse Zaken voor alarm- en camerasystemen nr. 1021.926.276

9. Belangrijke opmerking

Dit document beschrijft de beveiligingsmaatregelen van Ajax op basis van de informatie die de fabrikant publiceert. De beschikbare functies kunnen verschillen per model van de centrale. Ajax-systemen zijn ontworpen met een hoog beveiligingsniveau, maar geen enkel systeem kan absolute onkwetsbaarheid garanderen. Brepoels Security zorgt voor een correcte installatie en configuratie volgens de richtlijnen van de fabrikant.

Bronnen

1. Ajax Systems Support, "Jeweller radio protocol: technology and capabilities": ajax.systems/support/posts/jeweller-radio-protocol
2. Ajax Systems Support, "Hub encryption" (FAQ): ajax.systems/support/faqs/hub-encryption
3. Ajax Systems, "Ajax Systems' AES-128 encryption is now NIST-validated": ajax.systems/blog/nist-validation
4. Ajax Systems, "How OS Malevich updates": ajax.systems/blog/ajax-updating-procedure
5. Ajax Systems, "What is jamming of a wireless security system and how to resist it": ajax.systems/blog/what-is-jamming
6. Ajax Systems, Hub 2 user manual: ajax.systems/support/manuals/hub-2
7. Ajax Systems Support, "Accounts and permissions": ajax.systems/support/posts/accounts-and-permissions
8. Ajax Systems, "What is a security grade": ajax.systems/blog/what-is-a-security-grade
9. Ajax Systems, "Grade 3 certification": ajax.systems/blog/grade-3-certification
10. Ajax Systems, "Superior Hub Hybrid certified to ETSI EN 303 645": ajax.systems/blog/superior-hub-hybrid-certified-etsi-standard
11. Ajax Systems, "Ajax complies with the EN 18031 series of standards": ajax.systems/blog/ajax-complies-with-the-en-18031-series-of-standards

Brepoels Security · Bremakker 37, 3740 Bilzen · 089 39 08 99 · info@groupbrepoels.com · btw BE 1021.926.276
Vergunde onderneming FOD Binnenlandse Zaken voor alarm- en camerasystemen nr. 1021.926.276