백서

사이버 보안

개념 및 용어

목차

1. 소개

이 문서에서는 사이버 보안 개념 및 용어를 폭넓게 설명합니다. 이 문서의 내용은 단순화된 설명, 모델 및 구조에 기반해 있습니다. 대상자는 물리적 보안 시스템에 초점을 맞추고 사이버 보안의 기초를 이해하려는 개인과 단체입니다. 이 문서는 다른 Axis 사이버 보안 관련 문서의 용어 정의 참조 문서입니다.

2. 사이버 보안

사이버 보안은 여러 가지로 정의됩니다. 위키피디아(Wikipedia)에서는 컴퓨터 보안을 다음과 같이 정의하고 있습니다.

> *컴퓨터 보안은 사이버 보안 또는 IT 보안이라고도 하며 컴퓨터 시스템을 하드웨어, 소프트웨어 또는 컴퓨터 시스템에 저장된 정보의 도난 또는 손상으로부터 보호하고 그러한 컴퓨터 시스템이 제공하는 서비스의 중단 또는 오도로부터 보호하는 것입니다.*

온라인에서 안전을 유지하는 유일한 방법은 없습니다. 디지털 보안은 사용하는 도구와 관련된 것이 아니라 직면하는 위협과 그러한 위협에 대응할 수 있는 방법을 이해하는 것과 관련되어 있습니다. 보안성을 높이려면 무엇을 보호해야 하고 누구로부터 보호해야 하는지 결정해야 합니다. 위협은 어디에 있는지, 무엇을 하고 있는지, 누구와 함께 작업을 수행하고 있는지 하는 것에 따라 달라질 수 있습니다. 따라서 최상의 솔루션을 결정하려면 위협 모델링 평가를 수행해야 합니다.

3. 위험 평가

사이버 공간의 위험 분석 과정은 물리적 보호 환경의 위험 분석과 비슷합니다. 물리적 세계에서는 보호가 필요한 것은 일반적으로 물리적 사물, 건물 및 사람입니다. 사이버 공간에서는 자산은 정보/데이터이며 자원은 서비스입니다. 물리적 균열은 감지하기가 더 쉽고 도난과 손상은 더 많이 눈에 띕니다.

위험 평가 시의 다섯 가지 기본적 질문:

1. 무엇을 보호하고 싶습니까?
2. 누구로부터 보호하고 싶습니까?
3. 보호가 필요할 가능성은 어느 정도입니까?
4. 실패할 경우 결과가 얼마나 나쁩니까?
5. 그러한 결과를 방지하기 위해서 얼마나 많은 수고를 감당할 것입니까?

ISO 27000 정보 보호 표준에서는 자산의 **기밀성, 가용성** 및 **무결성**(또는 보안 삼각형이라고도 알려져 있는)에 대해 기술합니다.

데이터 또는 서비스에 액세스할 수 없을 경우, 데이터가 파손된 경우 또는 데이터가 승인되지 않은 당사자에게 공개될 경우 어떤 영향이 있습니까? 영향을 평가하려면, 데이터 유형마다 가치가 다를 수 있기 때문에 데이터를 분류해야 합니다.

ISO는 데이터와 서비스를 **접근 제한형(Restricted)**, **비공개형(Private)** 또는 **공용(Public)**으로 분류합니다. 예를 들어 하나의 비디오 시스템은 비디오 시스템 리소스를 다음과 같은 방법으로 분류할 수 있습니다.

> 라이브 비디오는 공용으로 분류됩니다. 이것은 일반인에게 공개되는 것일 수도 있고, 조직 내의 구성원에게 공개되는 것일 수도 있습니다. 라이브 비디오가 일반 대중에게 노출될 경우, 피해가 제한적입니다.

> 녹화된 비디오는 **비공개형**으로 분류될 수 있고, 특정 조직 단위만 액세스할 수 있습니다. 녹화된 사건 중 일부는 민감할 수 있기 때문입니다.

> 시스템 구성, 계정 및 암호는 **접근 제한형**으로 분류되고, 조직 내의 선택된 사람들만 액세스할 수 있습니다.

4. 보안 위협 환경

누군가 취약점을 활용하여 시스템을 공격하는 근본적인 이유가 항상 있습니다. 공격은 기회주의적 공격 또는 표적 공격으로 분류할 수 있습니다. 사이버 보안에서 공격자는 악의적 의도를 갖고 있을 수 있거나 무의식적으로(또는 우발적으로) 자산에 대한 피해를 유발할 수 있는 **적수**라고도 언급됩니다.

오늘날 발생하는 공격의 대다수는 기회주의적 공격, 즉 기회를 포착하여 이루어지는 공격입니다. 대다수의 경우에, 기회주의적 공격자들은 희생자가 누구인지 모릅니다. 이러한 공격자들은 개방형 네트워크, 서비스 및 포트의 스캐닝, 기본 또는 공통 암호의 입력 시도, 패치되지 않은 서비스 찾기, 피싱 이메일 전송과 같은 저비용 공격 벡터를 사용합니다. 기회주의적 공격자들은 실패한 공격에 시간이나 자원을 투입하려 하지 않고 다음 희생자로 이동합니다. 표준적인 수준의 보호를 적용하면 기회주의적 공격과 관련된 대다수의 위험이 완화됩니다.

특정 시스템을 겨냥하고 구체적 목표를 갖고 있는 표적 공격은 방어하기가 더 어렵습니다. 표적 공격은 기회주의적 공격과 동일한 저비용 공격 벡터를 사용합니다. 그러나, 초기 공격이 실패할 경우, 표적 공격자는 더욱 단호해지며, 얼마나 많은 가치가 훼손될 수 있는가 하는 것에 따라 더 정교한 방법을 사용하는 데 시간과 자원을 투여합니다. 표적 공격자는 종종 정교한 소셜 엔지니어링 및 스피어 피싱(특정 수신자를 겨냥한 이메일 공격)을 사용하여 시스템에 액세스합니다. 실패할 경우 표적 공격자는 시스템, 소프트웨어 또는 프로세스를 분석하여 이용 가능한 대안적 취약점을 찾습니다.

5. 위협 행위자 및 그 동기

어떤 행위자가 공격할 가능성이 가장 높은 행위자인지 어느 정도 이해하면, 공격자의 동기를 가정할 수 있고, 얼마만큼의 시간과 자원 그리고 의지를 투입할 것인지, 그리고 어떠한 취약점을 노릴 것인지 이해할 수 있습니다.

> **절친한 사람들** - 타인의 사생활을 꼬치꼬치 캐내려고 하는 사람들.

> **피고용인**, 또는 정당한 접근 권한을 갖는 사람들 - 우발적으로 또는 의도적으로 오용하는 사람들.

> **장난꾼** - 컴퓨터 시스템 간섭을 즐거운 놀이라고 생각하는 사람들.

> **핵티비스트** - 정치적 또는 이데올로기적 동기로 단체를 공격하려는 사람들.

> **사이버 범죄자** - 사기 또는 중요 정보의 판매를 통해 돈을 버는 데 관심을 갖는 사람들.

> **산업 경쟁자** - 자기 회사를 위해 경제적 우위를 확보하는 데 관심이 있는 사람들.

> **사이버 테러리스트** - 이데올로기적 또는 정치적 목표를 갖고 불안이나 공포를 유발하도록 고안된 공격을 수행하는 사람들.

> **국가**(해외 정보 수집 기관) - 경제적/정치적 이익을 얻기 위해서 또는 중요 정보 시스템을 손상시키기 위해서 활동.

> **개인들**, 개인들을 대신하여 행동하는 특정인 또는 특정 그룹 - 동기가 위에서 언급한 동기와 다를 수 있습니다. 탐사 저널리스트 또는 화이트햇 해커를 예로 들 수 있습니다. 결점과 취약점을 고치지 않고 숨기는 데 자원을 사용할 경우 화이트햇 해커(윤리적 해커)가 위협을 제기할 수 있습니다.

6. 공격의 가치 및 비용

공격의 가치는 공격 비용 대비 성공적 공격으로 얻는 이익에 따라 다릅니다. 사이버 보안의 목표는 공격 비용이 공격으로 얻는 이익보다 높아지게 하여 공격의 가치(가치 = 이익 – 비용)를 낮추는 것입니다. 적절한 보호 수준을 적용하려면(공격 비용을 파악하려면), 무엇이 가능한 위협인지 아는 것이 중요합니다. 모든 시스템이 위협 행위자 또는 공격 의도에 노출될 수 있지만, 일부 위협은 다른 위협보다 가능성이 높습니다. 어떤 위협의 가능성이 더 높은지 이해하면 어디에 초점을 두고 보안 조치를 취해야 하는지(어떤 취약점이 이용될 수 있는지) 파악하는 데 도움이 됩니다.

7. 공통적 조직 유형 및 위협

공격의 부정적 영향은 일반적으로 희생 조직의 유형에 따라 다릅니다.

조직 유형	**예**	**가능한 공격자**	**영향**
소규모 조직	> 소비자 > 가족 사업체 > 비영리	> 절친한 사람들 > 장난꾼 > 기회주의적 해커	**개인적** 수준 > 프라이버시 > 무결성
사업 조직	> 산업 > 기업 > 소매업체	위의 경우에서 추가적으로: > 피고용인 > 핵티비스트 > 조직 범죄자 > 경쟁자	**기업적** 수준 > 금전 손실 > 가동 정지 > 신뢰 > 지적 재산 > 경쟁 우위
중요 인프라 조직	> 에너지/수자원 > 은행/금융 > 통신 > 교통 > 공공 보건 > 경찰/군대	위의 경우에서 추가적으로: > 국가 > 사이버 테러리스트	**공개적** 수준 > 안전 > 공급 > 공포

8. 위험

사람마다 "위험"이라는 용어를 다르게 정의할 수 있습니다. RFC 2828 인터넷 보안 용어집(RFC 2828 Internet Security Glossary)에서는 위험을 다음과 같이 정의합니다.

특정 위협이 특정 취약점을 이용하여 특정한 유해한 결과를 얻을 확률로 표현되는 손실 예상.

다수의 상황에서 사용되는 약칭 버전은 위험 = *확률 * 영향.* 이 공식은 위협 유형들의 우선순위를 정하는 데 사용됩니다. RFC의 용어 정의에서는 "특정한"이라는 단어를 사용하여 위협, 취약점 및 유해한 결과를 설명합니다. 각 위협은 가장 가능성이 높고 부정적 영향이 가장 높은 위협부터 시작하여 개별적으로 조사해야 합니다.

각 보호 유형(기밀성, 가용성 및 무결성)의 경우, 위협의 부정적 영향을 어느 정도 이해하는 것이 중요합니다. 이 작업은 힘듭니다: 추정은 많은 경우에 주관적이며, 영향은 종종 과소 평가됩니다. ISO 27000 영향 유형(**제한적, 심각한, 중대한** 또는 **재앙적**)은 영향을 신속하게 파악하여 우선순위를 정하는 데 도움이 될 수 있습니다. 영향 유형을 복구에 걸리는 시간과 관련하여 생각할 수 있습니다. 제한적 = 시간/일, 심각한 = 주, 중대한 = 월, 재앙적 = 년 등으로 생각할 수 있습니다.

9. 보안 관리 조치

보안 관리 조치를 추가하는 과정을 보안 강화라고 합니다. 보안 관리 조치는 물리적 재산, 정보, 컴퓨터 시스템 또는 기타 자산에 대한 보안 위험을 방지, 감지, 대응 또는 최소화하는 데 사용되는 안전 장치 또는 대책입니다.

액세스를 제한하고 노출을 감소시키면 시스템의 사용성이 감소합니다. 시스템 사용성과 시스템 보호 간의 균형을 유지하려면 종종 시스템 사용자의 필요와 시스템 보호 담당자의 필요 사이의 힘든 타협이 필요합니다. 제한이 너무 많으면 사용자가 보호를 우회하는 방법을 찾아 새로운 취약점을 발견할 수도 있습니다. 사용성과 보호 필요 사이의 바람직한 균형은 시스템 소유자가 정의합니다.

10. 취약점 및 노출

취약점은 공격자에게 시스템에 액세스할 기회를 제공합니다. 취약점은 결함, 기능 또는 사용자 오류로 인해 발생할 수 있습니다. 공격자는 그러한 것들 가운데 하나를 이용하려 하고, 종종 그러한 것들을 한 개 이상 조합하여 최종 목표를 달성합니다.

조사 결과에 따르면 모든 성공적 공격의 95% 이상이 사람의 실수, 부실하게 구성된 시스템 및 부실하게 유지보수되는 시스템에서 기인합니다. 이러한 요소들은 일반적으로 적절한 정책 및 지정된 책임이 없어서 발생한 결과입니다.

장치 API(Application Programming Interface)와 소프트웨어 서비스에는 공격에서 이용될 수 있는 결함이 있을 수 있습니다. 어떤 벤더도 제품에 결함이 없다고 보증할 수 없습니다. 결함을 알고 있을 경우, 결함이 보완하는 보안 관리 조치로 위험을 완화시킬 수 있습니다. 한편, 공격자가 알려지지 않은 결함을 발견할 경우, 제로 데이 익스플로잇(zero-day exploits)이 발생하고 희생자에게 시스템 보호 시간을 주지 않을 수 있습니다.

중요하지 않은 취약점은 영향이 낮은 취약점, 또는 잠재적 영향은 심각할 수 있지만 이용하기 매우 힘든 취약점입니다. 중요 결함을 이용하려면 다수의 조건이 충족되어야 할 수도 있습니다. 이러한 조건들에는 네트워크 및 네트워크가 제공하는 리소스에 액세스할 권한을 갖는 것을 포함합니다.

일반적 취약점 점수 평가 시스템(Common Vulnerability Scoring System (CVSS))은 소프트웨어 취약점의 심각도를 분류하는 한 가지 방법입니다. CVSS는 취약점을 얼마나 쉽게 이용할 수 있고 어떤 부정적 영향이 있을 수 있는지 파악하는 공식을 사용합니다. 점수는 0점에서 10점 사이로 평가되며 10점일 경우 가장 심각한 것입니다. 공개된 일반적 취약점 및 노출(Common Vulnerability and Exposure (CVE)) 보고서에서 CVSS 점수를 볼 수 있습니다. Axis는 CVSS를 소프트웨어/제품에서 파악된 취약점이 얼마나 위험할 수 있는지 추정하기 위한 여러 조치들 가운데 하나로 사용합니다.

또한 노출은 취약점의 위험을 결정하는 데 일정한 역할을 합니다. 공격자가 취약점을 얼마나 쉽게 이용할 수 있는가? 이것은 인프라, 서비스 노출 및 일일 운영에 따라 다릅니다.
예: 취약점의 위험은 기업 비즈니스 포털 역할을 하는 공용 웹 서버에서는 심각한 위험으로 분류될 수 있습니다. 이러한 취약점은 로컬 보호 네트워크에서 카메라에서 사용될 때 제한적 위험으로 분류될 수 있습니다.

11. 취약점 스캐닝

취약점 스캐닝은 소프트웨어 또는 제품에 대한 자동 또는 수동 감사입니다. 여러 종류의 스캐닝 도구가 시장에 존재합니다. 취약점 스캐닝은 알려진 취약점을 갖는 서비스를 파악하는 데 사용됩니다. 그러한 서비스는 공격자에게 노출될 경우 공격자에 의해 이용될 수 있습니다.

취약점 스캐닝은 알려진 취약점만 찾을 수 있습니다. 취약점 스캐닝의 결과는 제품의 보안성에 대한 좋은 척도가 아닙니다. 새로운 중요한 취약점이 내일 발견될 수도 있습니다. 취약점 스캐닝은 때때로 침투 테스트와 혼동됩니다. 침투 테스트는 보안 관리 조치를 적극적으로 우회하려 할 때 이루어집니다. 취약점 스캐닝은 잠재적 취약점만 파악합니다.

12. IP 필터링

IP 필터링은 카메라의 로컬 방화벽 같은 역할을 합니다. 전문적인 비디오 시스템에서는 비디오 관리 시스템(VMS)이 시스템의 중심입니다. 비디오 클라이언트는 카메라에서 비디오에 직접 액세스하지 못합니다: 라이브 비디오와 녹화된 비디오는 VMS 서비스를 통해서 클라이언트에게 공급됩니다. 이것은 정상적 작동 중에 카메라에 액세스하는 유일한 컴퓨터/서버는 VMS 서버라는 것을 뜻합니다. 비디오 시스템이 비-비디오 클라이언트가 네트워크를 통해 카메라에 액세스할 수 있는 비격리 네트워크에 연결된 경우, IP 필터링을 추가적 보호로서 적용할 수 있습니다. IP 필터링의 경우, 카메라가 화이트리스트에 정의되지 않은 어떠한 IP 주소의 요청에도 응답하지 않습니다. 화이트리스트에는 VMS 서버, AXIS Camera Manager(ACM) 서버 및 고장 진단과 유지보수에 사용될 수 있는 기타 PC(있을 경우)가 포함되어야 합니다.

13. 네트워크 격리 (네트워크 분할)

네트워크 격리는 중요한 네트워크 자원을 서로 분리하여 서로 부정적 영향을 줄 위험을 줄이는 방법입니다. 격리는 서로 상호작용할 필요가 없는(또는 상호작용해서는 안 되는) 리소스들에 특히 적합합니다. 네트워크 분리는 가상일 수 있습니다(VLAN). 이것은 관리형 스위치의 인프라를 요구합니다. 또한 네트워크를 다른 케이블 배선 및 네트워크 기어를 사용하여 격리할 수 있습니다. 사용할 분리 유형은 비용, 인프라 및 정책에 따라 다릅니다.

전체적으로 좋은 보호는 물리적 보안 네트워크를 다른(도메인) 네트워크 리소스들과 격리하는 것입니다. 한 네트워크의 비디오 클라이언트가 다른 세그먼트의 VMS 서버에 액세스할 필요가 있을 경우 두 세그먼트 사이에 방화벽을 추가할 수 있습니다. 방화벽은 클라이언트와 VMS 서버(카메라로 전송되는 트래픽이 아니라) 사이에서만 개방되어야 합니다.

14. 네트워크 암호화 – HTTPS

네트워크 암호화는 클라이언트, VMS 및 카메라 사이의 통신을 보호하고, 네트워크 트래픽 스니핑을 이용한 정보 추출을 방지하며, 전송 중의 데이터 변경을 방지합니다. 네트워크 암호화가 카메라, VMS 또는 클라이언트에 대한 보호를 반드시 높여주는 것은 아닙니다.

Axis 카메라는 HTTPS(보안 SSL/TLS 터널을 통한 HTTP)를 지원합니다. 클라이언트(예를 들어 VMS)도 HTTPS를 지원해야 합니다. HTTPS는 모든 관리 트래픽(정상적 HTTP 트래픽)을 암호화하지만 반드시 비디오를 암호화할 필요는 없습니다. 왜냐하면 비디오는 RTSP(Real-Time Streaming Protocol)를 통해 전송되기 때문입니다. 비디오를 암호화하려면 VMS도 암호화된 TLS 터널을 통해 터널링되는 RTSP 요청을 지원해야 합니다. 모든 VMS가 이것을 지원하는 것은 아닙니다. VMS 벤더에게 확인하십시오. HTTPS가 설정되기 전에 카메라가 인증서(자가 서명되거나 CA가 서명한)를 가져야 하고 HTTPS 정책이 설정되어야 합니다.

15. 인증 기관 (CA)

자가 서명 인증서를 사용하든 CA가 서명한 인증서를 사용하든 암호화 수준에는 차이가 없습니다. 차이가 있다면 자가 서명 인증서는 네트워크 스푸핑(공격 컴퓨터가 정상적 클라이언트 또는 서버로 위장하려 하는 상황)을 방지하지 않는다는 것입니다. CA가 서명한 인증서는 신뢰되는 카메라에 액세스하고 있음을 클라이언트가 인증하기 위한 트러스트포인트를 추가합니다. CA가 서명한 인증서는 HTTPS(**서버 인증서**)와 802.1x(**클라이언트 인증서**) 모두에 사용됩니다.

공개 CA vs. 사설 CA

Comodo 및 Symantec(이전의 Verisign)과 같은 공개적으로 신뢰되는 CA는 일반적으로 공용 웹사이트 및 이메일 서버와 같은 공용 서비스에 사용됩니다. 공개적으로 신뢰되는 CA용 CA 루트 인증서는 대다수 운영 체제(Windows, Linux, Mac)와 브라우저에 미리 설치되어 있습니다.

사설 CA는 내부/사설 네트워크 서비스용 트러스트포인트입니다. 사설 CA는 모든 내부 클라이언트 및 서버용 인증서를 발행하는 데 사용되는 소프트웨어/서버(일반적으로 Active Directory/Certificate Service)입니다. 사설 CA 루트 인증서를 사설 리소스에 액세스하는 모든 클라이언트에 설치해야 합니다. 인증서는 사용 가능한 도구 및 인프라에 따라 수동으로 또는 자동으로 배치할 수 있습니다.

16. 네트워크 액세스 제어 – 802.1X

IEEE 802.1X는 승인되지 않은 네트워크 장치가 로컬 네트워크에 액세스하는 것을 방지하도록 고안된 표준입니다. 장치는 네트워크(및 그 리소스) 액세스가 허용되기 전에, 자체 인증을 해야 합니다. MAC 주소(MAC 필터링), 사용자/암호 또는 클라이언트 인증서와 같은 여러 인증 방법을 사용할 수 있습니다. 시스템 소유자는 사용할 방법을 결정합니다. 적절한 선택은 위협, 위험 및 비용에 따라 다릅니다.

802.1X 인프라 운영은 투자입니다. 관리형 스위치와 추가 서버, 일반적으로 RADIUS(Remote Authentication Dial-In User Service)가 필요합니다. 클라이언트 인증서를 사용하려면 클라이언트 인증서를 발행할 수 있는 CA(사설 또는 공용)가 필요합니다. 대부분의 경우, 인프라는 유지보수 및 모니터링 인력을 필요로 합니다. 최종 사용자가 기존에 802.1X 인프라를 사용하고 있지 않을 경우, 네트워크 비디오/보안 시스템이 추가될 때 802.1X 인프라가 추가될 가능성은 적습니다. 802.1X의 대안을 제공할 수 있는 보완적 관리 조치는 네트워크를 격리하여 다른 중요 네트워크 리소스의 노출을 줄이는 것입니다.

17. SNMP

SNMP(Simple Network Management Protocol)는 IP 네트워크의 관리형 장치에 대한 정보를 수집하고 정리하는 데 사용됩니다. SNMP를 사용하여 카메라를 모니터링하면 공격을 받았을 수도 있음을 나타낼 수 있는 카메라 오작동 및 연결 끊김을 감지하는 데 도움이 될 수 있습니다.

18. Syslog 서버

모든 카메라에는 카메라의 모든 동작을 기록하는 내부 로그가 있습니다. 내부 로그는 카메라를 재부팅할 경우 소실될 수 있으며, 또는 공격자가 침입 공격을 하여 내부 로그를 삭제하거나 변경할 수 있습니다. 원격 Syslog 서버는 일상 운영 중의 모든 카메라 로그 메시지를 수집할 수 있습니다. 원격 Syslog 서버를 사용하면 로그 보안이 유지됩니다. 따라서 문제 해결, 또는 비정상 및 침입 흔적을 찾기 위한 과학 수사를 단순화할 수 있습니다.

19. 상세 정보:

www.axis.com/support/product-security

> AXIS 취약점 정책

> AXIS 보안 강화 가이드

> 보안 권고(CVE)

> 백서

www.axis.com/learning/online-courses

> AXIS Academy 사이버 보안 교육

www.axis.com/blog/secure-insights/category/cyber-security

> 사이버 보안에 대한 다양한 블로그 포스팅

71007/KO/R1/1708

Axis Communications에 대하여

네트워크 비디오 분야의 선도 기업인 Axis는 보다 스마트하고 안전한 세상을 위한 지능형 보안 솔루션을 제공합니다. 업계 리더로서 Axis는 개방형 플랫폼에 기반한 혁신적인 네트워크 제품을 지속적으로 출시하여 시장의 성장을 이끌어 가고 있으며, 글로벌 파트너 네트워크를 통해 고객에게 한 차원 높은 가치를 제공하고 있습니다. Axis는 파트너들과 신뢰를 바탕으로 한 공고한 관계를 장기간 유지하고 있으며 기존 및 신규 시장에서 새로운 수요를 창출할 수 있도록 파트너들에게 전문 지식 제공과 함께, 혁신적인 네트워크 제품을 공급하고 있습니다.

Axis는 전 세계 50개 이상의 국가에 지사를 두고 2,700명 이상의 직원이 일하고 있으며, 90,000곳 이상의 파트너로 구성된 글로벌 네트워크를 보유하고 전세계 고객들에게 최상의 제품과 서비스를 제공하고 있습니다. 1984년에 설립된 Axis는 스웨덴에 본사를 두고 있으며 현재 NASDAQ Stockholm에 상장(AXIS)되어 있습니다.

Axis에 대한 보다 자세한 정보는 www.axis.com에서 확인하실 수 있습니다.

AXIS COMMUNICATIONS