표준 사이버 보호

컴퓨터 네트워크는 끊임없이 공격 받고 있습니다. 그러나 이러한 공격의 극히 일부만 성공을 거둡니다. 사이버 공격의 대다수는 우발적이며, 특정 피해자를 대상으로 하지 않고 단순히 개방된 네트워크/포트를 찾아 들쑤시고 다니면서 추측하기 쉬운 패스워드를 시도하고, 패치가 안 된 네트워크 서비스를 선택해 피싱 사기 이메일을 보냅니다. 공격자들은 실패한 공격에 시간을 허비하거나 노력을 쏟으려 하지 않고, 다음 잠재적 피해자를 찾아 옮겨갈 뿐입니다.

공격자를 잠겨있지 않은 차량을 발견할 때까지 거리에서 배회하며 차량 손잡이를 열어보는 차량 절도범이라고 가정한다면, 다음의 몇몇 표준 사이버 보안 강화 권장 사항을 따르는 것으로 우발적인 공격으로부터 쉽게 보호할 수 있습니다 – 이를테면, 차량의 문을 잠그지 않은 채로 두지 마십시오! 방화벽이 내장된 라우터 사용, 컴퓨터에 추측하기 어려운 패스워드 사용, OS 및 소프트웨어의 꾸준한 업데이트 등은 가정에서 할 수 있는 간단한 방법입니다. 다른 방법들은 지난 10~20년 동안 우리에게 주입되어 온 것들입니다. 즉, 모르는 발신자가 보낸 첨부 파일은 열지 마십시오, 악성 프로그램 방지 소프트웨어를 설치하십시오, 신뢰할 수 없는 사이트의 소프트웨어를 설치하지 마십시오, 거리에서 주운 USB 스틱을 PC에 연결하지 마십시오(어디에 있던 USB인지 알 수 없다고 엄마가 말해준 적 있지 않나요?)

여기는 Axis 블로그입니다. 그럼 IP 카메라에 대한 내용과 설치할 때 발생할 가능성이 있는 위험에 대해 알아볼까요? 다행히 카메라는 PC와 같은 수준의 위협 대상이 아닙니다. 카메라에는 로그인해 소프트웨어를 설치하고 웹 페이지를 방문하거나 이메일 첨부 파일을 여는 사용자가 없습니다. 다만 카메라에는 공격자가 다른 공격을 위한 '플랫폼'으로 사용하고자 할 수 있는 서비스가 있습니다. '사물 인터넷(IoT)'의 폭발적인 증가는 카메라를 포함하여 해커 그룹이 봇넷에서 '조종 대상'으로 만들기 쉬운 보안 수준이 낮고 인터넷에 많이 노출된 장비를 양산했습니다.

그래서 우발적 공격자의 위험을 완화시킬 몇 가지 간단한 권장 사항을 소개하겠습니다.

네트워크 노출 감소

기본적으로 꼭 필요하지 않은 이상 인터넷에 무언가를 연결하지 마십시오. 만약 연결해야 한다면, 실행 전에 시작 단계에서 보안 수준을 충분하게 높여야 합니다.

네트워크 카메라의 문제는 많은 사람들이 원격으로 비디오에 액세스하려고 한다는 것입니다. IP 카메라에는 종종 웹 브라우저만 이용해도 접근할 수 있는 웹 서버와 비디오가 있습니다. 라우터/방화벽의 허점을 찾는 것(포트 포워딩이라고도 함)과 자주 사용하는 비디오 클라이언트로 웹 브라우저를 사용하는 것이 좋은 생각처럼 보일 수도 있지만, 불필요한 위험을 가져오기 때문에 권장하지 않습니다.

개방성을 위해 Axis 카메라는 역사적으로 UPnP NAT 횡단, 라우터 포트 포워딩 구성 절차를 간소화하는 서비스를 지원해 왔습니다.

그러나 이는 기본적으로 사용할 수 있는 것은 아니며, 기본 지원도 권장하지 않습니다. 나중에 출시될 제품에서는 제거될 레거시 기능입니다. 원격으로 비디오에 접근할 수 있는 더 다양하고 향상된 보안 방법이 있습니다. VMS(비디오 관리 시스템)가 없는 개인 및 소규모 조직에 Axis는 무료 AXIS Companion 클라이언트 사용을 추천합니다. AXIS Companion을 이용하면 장치인 카메라를 인터넷에 노출하지 않고도 보안된 원격 비디오 액세스가 가능합니다. VMS를 사용하는 시스템에서는 원격 비디오 액세스에 대한 VMS 벤더의 권장사항을 따르십시오. 비디오가 공개적으로 스트리밍되는 경우(예: 웹을 통한 사용자 유인), 올바르게 구성된 인터넷 웹 서버에서 미디어 프록시를 사용할

것을 권장합니다. 그리고 원격 사이트가 여러 개인 경우, VPN(가상 사설 네트워크)을 사용하는 것이 가장 좋습니다.

추측하기 어려운 패스워드

대부분의 다른 인터넷 활성 장치와 같이, 카메라에 사용되는 패스워드는 데이터와 서비스에 승인되지 않은 액세스를 차단하는 주요 보호 수단입니다. 무엇이 강력한 패스워드인지에 대해 많은 논란이 있습니다. 일반적인 권장사항은 대/소문자, 숫자 및 특수 문자가 혼합된 8자리 이상의 패스워드를 사용하는 것입니다. 무작위 로그인 공격은 공격 시간이 아무리 길어도 강력한 패스워드에서 실효성이 없습니다. VMS 환경에서는 사용자가 카메라에 직접 액세스하지 않기 때문에 인증은 주로 기계 간에 이루어집니다. VMS 환경에서 로그인 실패 지연(login-failure-delay) 기능을 추가하면 사용자 스스로가 접근이 막히는 위험이 증가할 수도 있습니다. 더 작은 규모의 조직에서 클라이언트는 종종 카메라(인간과 기계 간 인증)에 직접 연결하므로, 추측하기 어렵지만 기억하기 쉬운 패스워드 사용을 권장합니다. “this is my camera passphrase(이것은 나의 카메라 패스프레이즈입니다)”와 같이 패스워드로 긴 패스프레이즈를 사용하십시오. 네, 패스워드에 공백이 허용됩니다. 어떤 것을 사용해도 상관없지만, 공장 초기화 패스워드는 사용하지 마십시오.

펌웨어 및 소프트웨어 패치

소프트웨어는 사람이 만들고 사람은 여전히 실수를 합니다(지금은요!). 그래서 소프트웨어가 실행되기 전에 취약성을 찾아내기 위해 최선을 다하고 있음에도 불구하고, 새로운 취약성은 주기적으로 발견되며 앞으로도 계속 그럴 것입니다. 대부분은 그렇지 않지만 일부 취약성은 치명적이므로, 항상 펌웨어 및 소프트웨어를 업데이트하고 주기적으로 새로운 버전을 확인하십시오. 치명적인 취약성이 발견되면 누구에게는 부당하게 이용할 좋은 기회가 생긴 것이므로, 경제적 이익을 위해 실행에 옮길 수 있습니다. 공격자가 패치되지 않은 네트워크 서비스에 접속하면 성공할 가능성이 높기 때문에, 이러한 침입 기회를 줄이는 것이 중요합니다.

표적 공격

기업 및 주요 기반 시설 조직은 우발적이기보다는 대상이 명확한 표적 공격에 노출되어 있습니다. 이는 전과 같이 동일한 저비용 매개를 사용하겠지만 명확한 대상을 목표로 하는 공격자의 경우 성패에 따라 더 큰 가치가 달려 있으므로 더 많은 시간, 리소스 및 투지를 동원합니다. 어떤 보안 제어를 사용하여 위험을 줄일지를 결정하기 위해 위협 모델링과 위험 분석에 착수하는 것이 좋습니다. 이 주제는 다음 블로그 포스트에서 더 자세하게 다룰 예정입니다.

Axis의 책임

Axis는 개발 절차 및 제품 수명 주기 향상, 더 효과적인 보안 제어, 더 많은 보안 기본 구성, 강화된 사용자 인터페이스 및 본 블로그 포스트와 같은 추가 정보를 제공하며 고객의 위험을 줄이기 위해 계속 노력하고 있습니다. IP 카메라의 보안을 강화하는 가장 좋은 방법에 대해 자세히 알아보려면, 이 가이드를 읽고 추가 권장 사항을 참조하십시오.