사이버 보안을 강화하는 방법

사이버 보안
안전한 네트워크를 위한
10가지 모범 사례

AXIS COMMUNICATIONS

소개

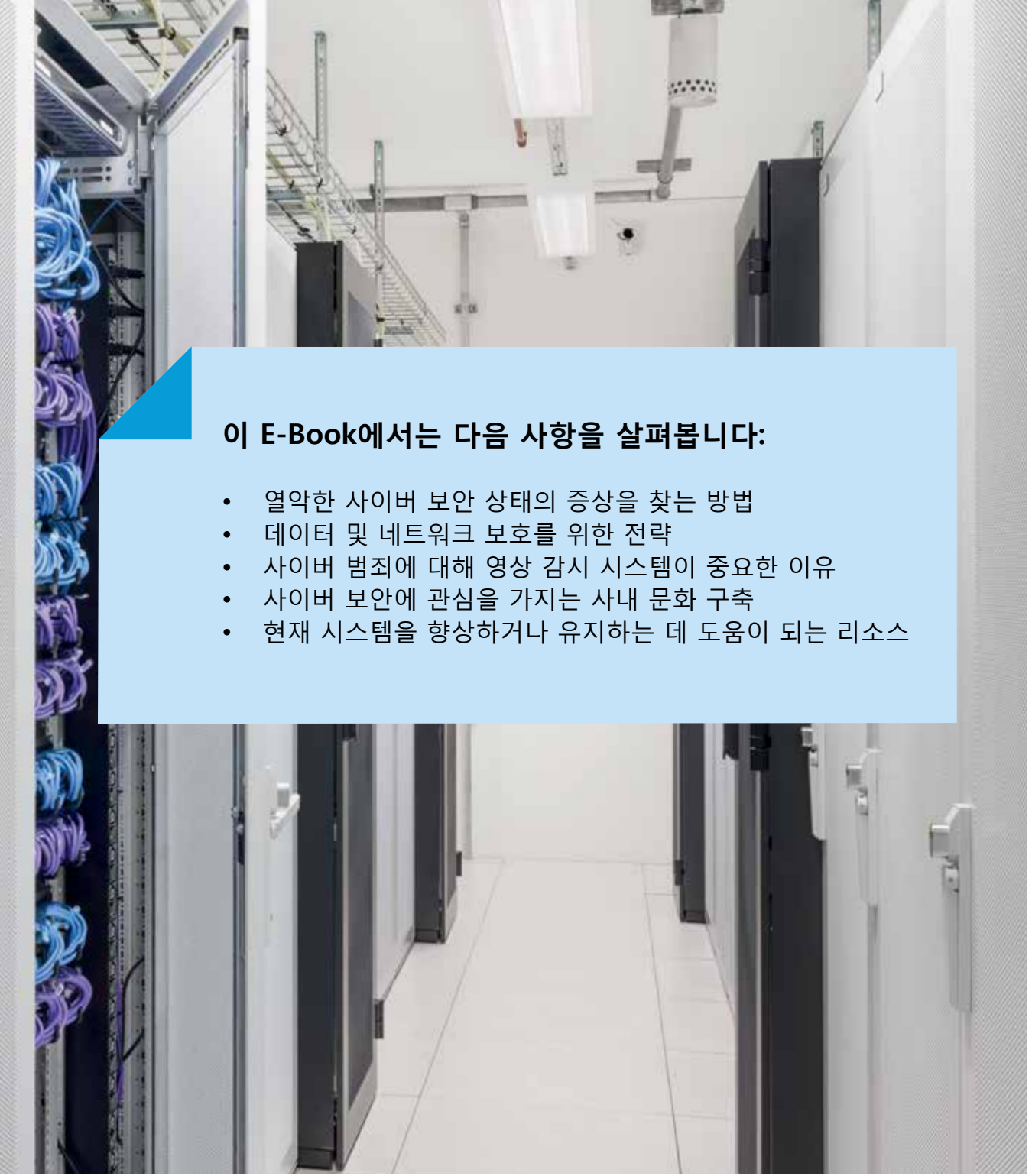
사이버 공격이 헤드라인 뉴스를 장식하는 빈도가 늘어남에 따라, 사이버 보안이 가장 먼저 떠오르는 것은 놀랄 일이 아닙니다. 비즈니스에 대한 사이버 보안 위협은 사상 최고이며, 빈도와 정교함 수준이 증가하고 있습니다.

그러나 최근 통계에 따르면 많은 조직이 기존의 위협 또는 서서히 나타나는 새로운 위협에 대해 대비하지 않고 있으며, CIO 및 CISO 중 3분의 2는 조직이 사이버 보안을 최우선 순위로 여기지 않는다고 말합니다.* 그러나 좋은 소식은, 사이버 취약점을 이해하고 이러한 취약점을 제한할 계획을 수립하여 실행하면 대부분의 공격을 막을 수 있다는 것입니다.

귀하의 조직은 정보 보안에 대해 효율적으로 계획하고 있습니까? 침해가 발생할 경우 사이버 보안 사고 대응 전략이 있습니까? 사이버 보안 정책에 대해 직원들을 적극적으로 교육하고 있습니까?

취약점을 찾고 안전한 네트워크 보안 상태를 보장하는 방법을 아는 것은 사이버 회복에서 중요한 측면입니다. 그러나 위협으로부터 네트워크를 보호하면서 동시에 네트워크가 필요한 사람들이 해당 네트워크에 액세스할 수 있게 하는 것은 매우 어려운 일입니다. 따라서 열악한 네트워크 보안 상태의 증상을 식별하고 네트워크의 보안 향상에 대해 사전 대책을 강구하는 것이 매우 중요합니다.

* 2015 Global Megatrends in Cybersecurity" Ponemon Institute LLC – condected by Raytheon



이 E-Book에서는 다음 사항을 살펴봅니다:

- 열악한 사이버 보안 상태의 증상을 찾는 방법
- 데이터 및 네트워크 보호를 위한 전략
- 사이버 범죄에 대해 영상 감시 시스템이 중요한 이유
- 사이버 보안에 관심을 가지는 사내 문화 구축
- 현재 시스템을 향상하거나 유지하는 데 도움이 되는 리소스

물리적 보안과 마찬가지로, 효과적인 사이버 보안은 취약점 식별, 위협 평가, 적절한 조치가 지속적으로 순환되는 것입니다.
네트워크를 강력하게 보호해야 할 필요성이 매일 더 분명해집니다. 강력한 방어를 보장하려면 네트워크뿐만 아니라 네트워크에 연결된 모든 장치에서도 보안 강화를 고려하십시오.
귀사의 네트워크는 가능한 최고의 수준으로 안전합니까?

열악한 네트워크 보안 상태의 증상 찾기

귀사에 사이버 위협을 사전 예방적으로 모니터링하여 대응하는 정책, 프로세스 및 인력으로 뒷받침되고 있는 강력하고 강화된 네트워크가 있고,

- 조직의 명시된 사이버 보안 목표에 부합되어 있는 경우,
- 귀사의 네트워크 보안 상태가 매우 좋은 것입니다! 사이버 보안에 대한 관심이 높고 위험이 증가하고 있는 상황에서, 귀사의 환경이 이러한 상태가 아니라면 곤란한 상황에서 벗어나기 위한 적절한 조치를 취해야 합니다.

보안이 제대로 구현되지 않은 네트워크는 해커에게 매우 매력적이며, 많은 경우 바이러스, 멀웨어(악성 소프트웨어) 및 기타 사이버 위협이 빠르게 퍼질 수 있습니다. 그러나 네트워크에서 활동 중인 사용자가 많이 있는 경우 생산성에 영향을 주지 않으면서 높은 수준의 보안을 유지하기 어렵습니다.

귀하 및 귀사의 네트워크는 공격에 대비하고 있습니까? 사이버 보안이 향상되어야 하는지 여부를 알아내는 몇 가지 방법을 살펴보겠습니다. 증상이 발견되고 평가되면, 일관된 사이버 보안 계획을 구축하기 위한 정책과 절차의 수정에 착수할 수 있습니다.

1

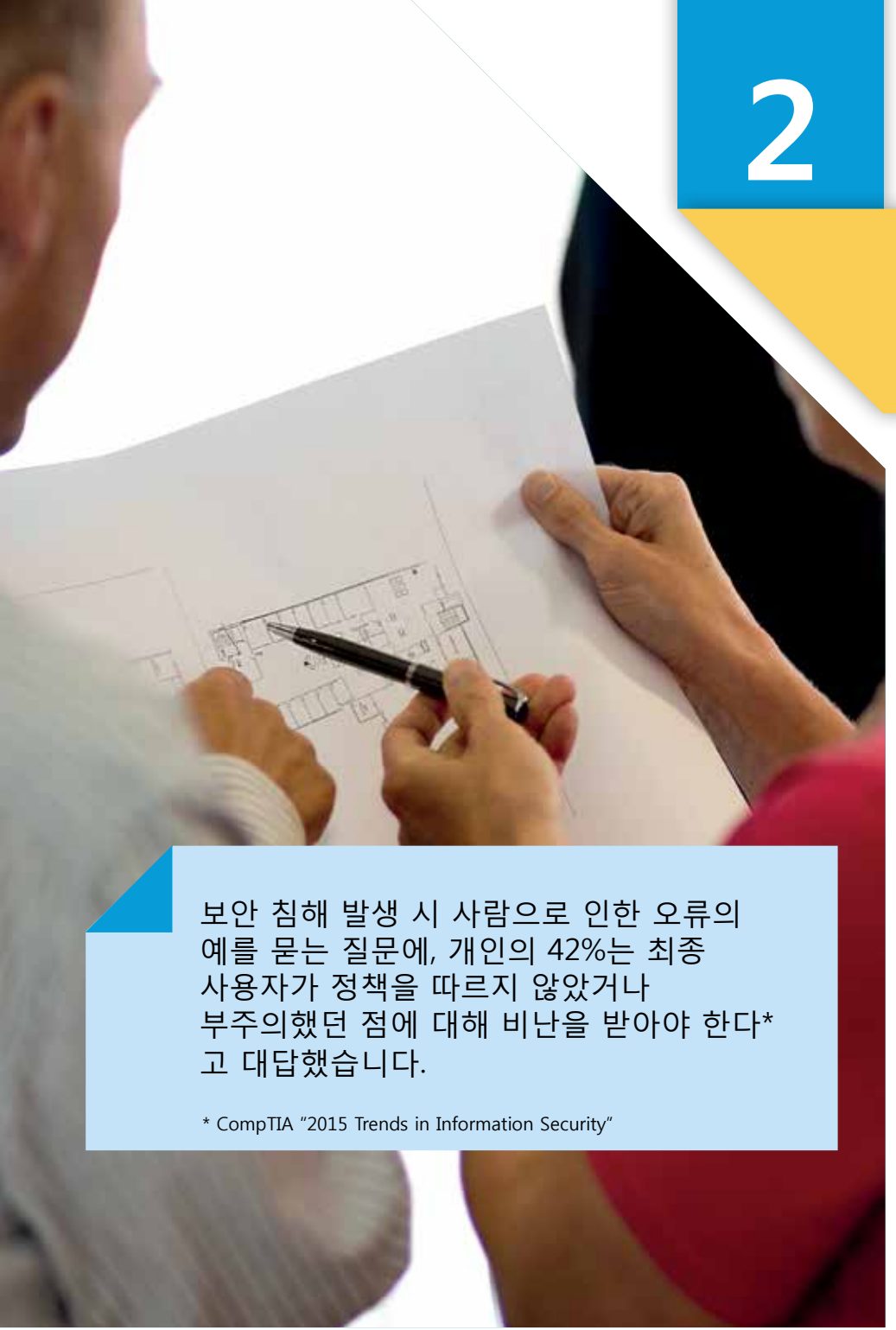
IT 팀과 보안 팀이 서로 연계되어 있지 않습니다.

Al Gore에 의해 인터넷이 발명된 이래로, 귀사의 IT 팀은 사이버 보안에 대해 생각해 왔을 것입니다.* 패스워드 관리 및 표준 네트워크 프로토콜과 관련하여 네트워크 운영에 대한 IT 정책이 있을 수 있습니다. 그러나 그 IT 정책이 IP 감시 네트워크에 적용되지 않고 있을 수 있습니다.

IT 팀과 사고 예방팀의 생각이 일치하지 않는 경우가 종종 있지만, 특히 사이버 보안과 관련된 경우에는 두 팀의 생각이 일치되는 것이 중요합니다. 일치되지 않은 몇 가지 분명한 징후는 다음과 같습니다.

> 상이한 네트워크에 대한 정책 및 프로세스의 차이 또는 부족
> 부실하거나 분명하지 않은 패스워드 관리
> 모든 시스템의 보안 조치를 검토하기 위한 오너십 또는 책임 부족
> 네트워크를 통해 전송되는 비디오 스트림에 대해 최신 고급 암호화 방법이 사용되지 않음
> 네트워크에 연결된 하드웨어 및 소프트웨어가 IT 정책에 부합되지 않음

* 예, 실제로 그가 인터넷을 발명하지 않았지만 요점을 이해하리라 생각합니다.



보안 침해 발생 시 사람으로 인한 오류의 예를 묻는 질문에, 개인의 42%는 최종 사용자가 정책을 따르지 않았거나 부주의했던 점에 대해 비난을 받아야 한다* 고 대답했습니다.

* CompTIA "2015 Trends in Information Security"

2

네트워크 사용자가 정책 및 절차를 따르지 않거나 그에 대해 모르고 있습니다.

정책과 절차가 마련되어 있습니까?
모든 사용자가 이해하기 쉽게 문서화되어 있습니까?

IT 팀에게 전하는 팁!
귀사의 IT 정책을 시행하고, 회사 컴퓨터 및 서버에 적용되었는지를 확인하십시오.

'아니요'라고 대답하는 경우, 이 열악한 네트워크 보안 상태 증상에 대한 희생자가 될 수 있습니다. 다음은 이 증상을 진단할 수도 있는 몇 가지 추가 질문입니다.

> 귀사의 직원들이 IT 정책에 대한 교육을 정기적으로 받고 있습니까?
> 새로운 직원이 들어올 경우, 해당 직원도 적절한 교육을 받습니까?
> 장치 패스워드와 관련하여, 직원을 위한 특정 지침이 있습니까?

3

설치 및 유지보수 계획이 분명하게 문서화되어 있지 않습니다.

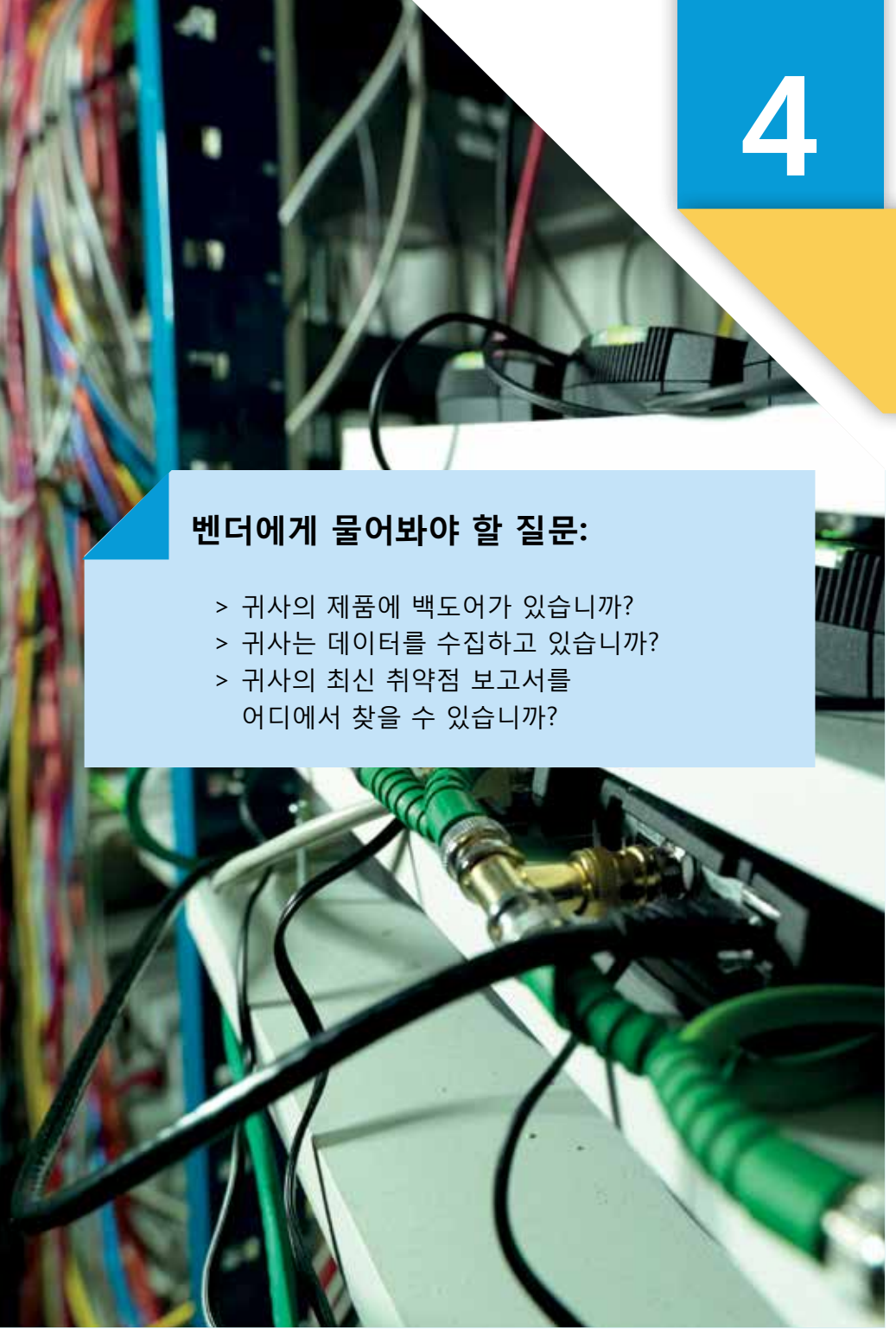
사이버 보안과 관련하여, 물리적 설치(IP 감시 카메라 또는 기타 네트워크 장치의 설치) 및 유지보수 문제도 우려의 원인이 될 수 있습니다. 설치 시 귀사가 요구한 특정 요구 사항을 설치업체가 이해하지 못하는 경우가 종종 있습니다. 관련 벤더가 너무 많은 경우, 설치업체가 각 벤더의 보안 모범 사례의 일부 또는 전부를 놓칠 수 있습니다.

더욱 심각한 것은, 유지보수 계획에 대해 보안, IT, 설비 및 유지보수 부서의 의견이 서로 일치되지 않는 경우를 너무 자주 보아왔다는 것입니다. 아마도 시스템에 대한 일상적인 유지보수조차 함께 수행하고 있지 않을 것입니다.

모든 네트워크 연결 장치의 설치 및 유지보수와 관련하여 문서화된 계획이 있습니까?

"처음 어떤 일을 올바르고 수행하는 데 마찰이 있다는 것은 그 일이 얼마나 어려운지에 대해 아무도 제대로 인식하지 못한다는 것입니다."

- Walter J. Wright



4

기술 벤더가 사이버 보안에 대해 이야기하지 않습니다.

선택한 장비가 귀사의 IT 정책에 들어맞습니까?
또는 벤더에 대해 귀사의 정책을 적용하고 있습니까?
현명하게 선택하십시오!

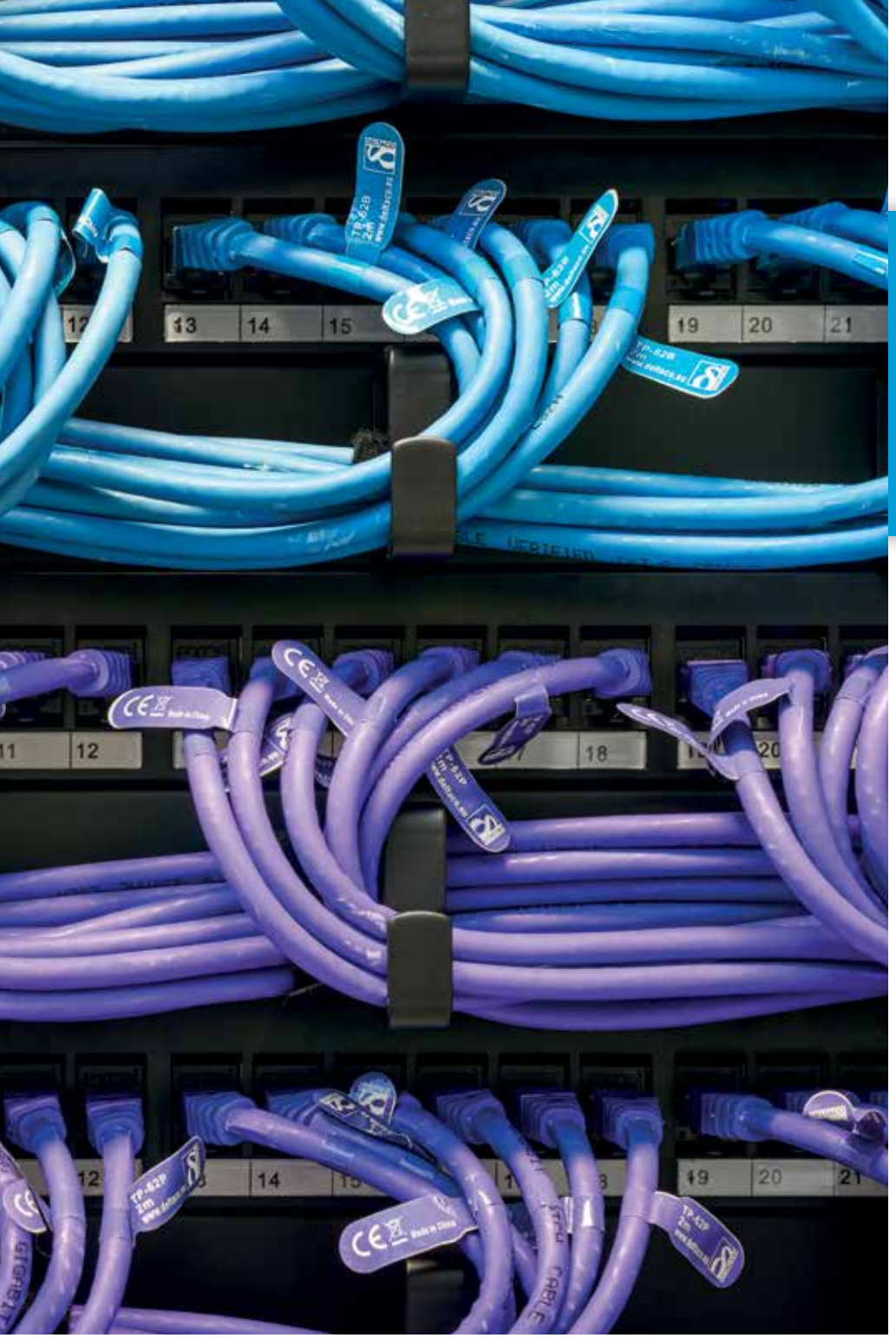
기술 벤더에 대한 경고 징후에는 다음 사항이 포함됩니다.

> 사이버 보안에 대해 이야기하지 않습니다.
> 장치 보안 강화 가이드 또는 모범 사례 가이드가 없습니다.
> 자사 제품에 대해 침투 테스트를 수행하지 않습니다.
> 자사 제품 위험을 평가하기 위해 써드파티 사이버 보안컨설턴트와 작업하지 않습니다.

각각의 기술은 더 큰 시스템의 일부이며, 시스템이 완전히 보호되지 않는 경우가 종종 있습니다. 에코시스템의 일부만 안전하고 나머지는 보호되지 않을 수 있습니다. 귀사의 보안 수준은 가장 약한 부분만큼만 강할 뿐입니다. 퍼즐의 각 부분이 최대한 안전하게 보호되고 있습니까?

벤더에게 물어봐야 할 질문:

> 귀사의 제품에 백도어가 있습니까?
> 귀사는 데이터를 수집하고 있습니까?
> 귀사의 최신 취약점 보고서를 어디에서 찾을 수 있습니까?



안전한 네트워크를 위한 10가지 모범 사례

지금까지 열악한 사이버 보안 상태를 찾는 방법을 알아보았습니다. 그럼 이제 귀사 네트워크의 사이버 보안을 향상하기 위해 무엇을 해야 하는지를 살펴보겠습니다. IT, 보안 및 설비 관리 팀과 함께, 여러 공통 위험을 완화하기 위한 작업을 할 수 있습니다.

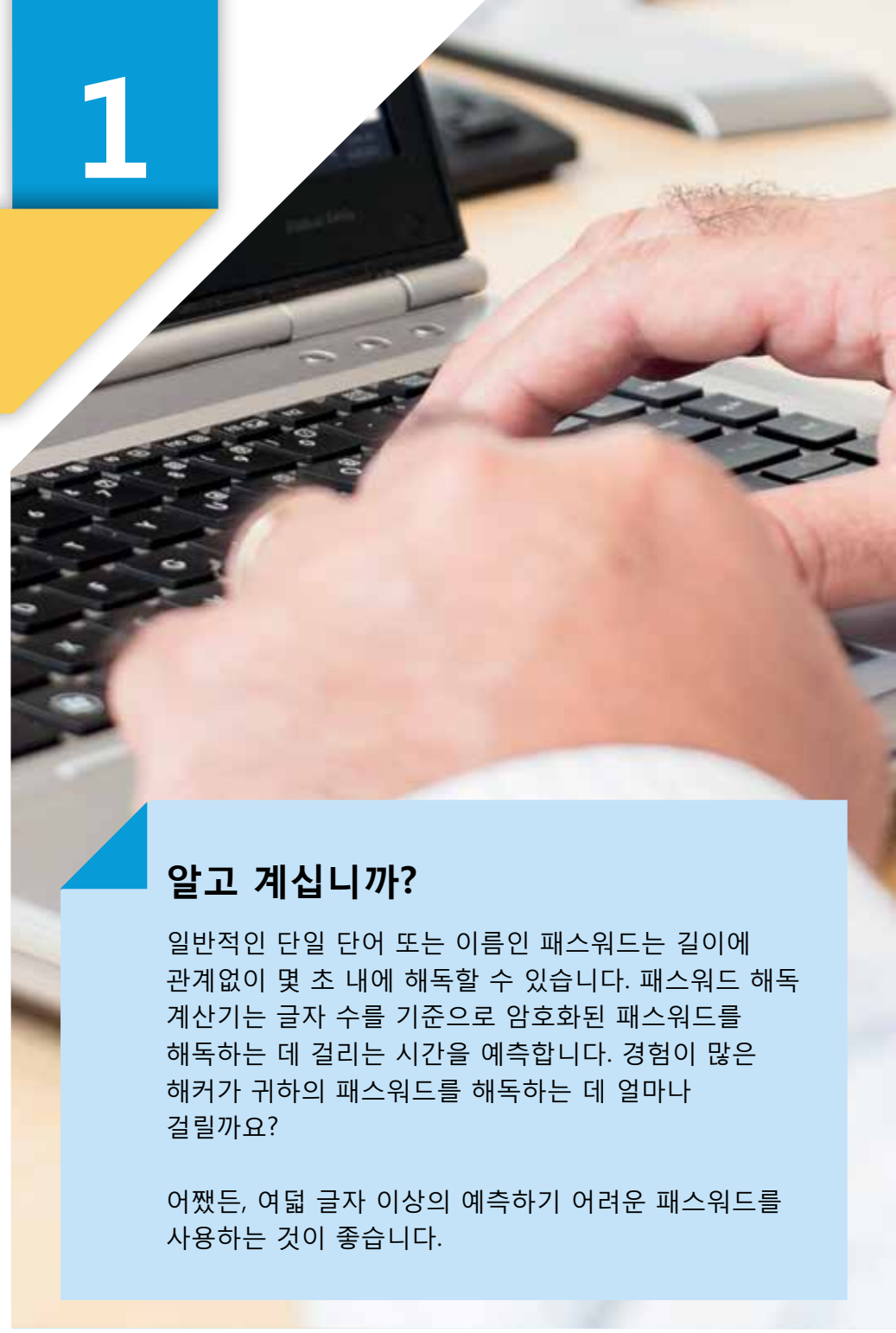
1

강력하고 독특한 패스워드를 사용하십시오.

대부분의 IP 기반 장치는 기본 패스워드와 기본 설정이 있는 상태로 제공됩니다. 이러한 패스워드는 예측하기 쉬우며, 온라인에 게시된 경우도 있습니다. 이는 사이버 범죄자가 시스템에 대한 무단 액세스할 수 있는 가장 일반적인 방법입니다.

패스워드를 활용하여 공격을 막는 가장 효율적인 방법은 다음과 같습니다.

> 강력하고 독특한 패스워드 설정
> 확실한 패스워드 관리
> 패스워드 대신 인증서 사용
> 정기적으로 패스워드 변경



알고 계십니까?

일반적인 단일 단어 또는 이름인 패스워드는 길이에 관계없이 몇 초 내에 해독할 수 있습니다. 패스워드 해독 계산기는 글자 수를 기준으로 암호화된 패스워드를 해독하는 데 걸리는 시간을 예측합니다. 경험이 많은 해커가 귀하의 패스워드를 해독하는 데 얼마나 걸릴까요?

어쨌든, 여덟 글자 이상의 예측하기 어려운 패스워드를 사용하는 것이 좋습니다.

2

권장 방식으로 장치를 배포하고 설치하십시오.

장치를 배포할 때, 사용하지 않은 서비스를 활성 상태로 유지하면 공격에 취약할 수 있습니다. 예를 들어, 사이버 범죄자는 신뢰할 수 없는 개발자의 FTP(파일 전송 프로토콜) 또는 애플리케이션 플랫폼을 사용하여 악성 애플리케이션과 스크립트를 설치할 수 있습니다. 사용하지 않은 서비스를 비활성화하고 신뢰할 수 있는 애플리케이션만 설치하면, 가해자가 시스템 취약점을 악용할 가능성이 감소됩니다.

또한 장치를 올바르게 설치하면 보안 문제를 방지할 수 있습니다. 예를 들어, 사람의 손에 닿는 위치에 카메라를 배치하면 카메라가 조작되거나 파손될 위험이 있습니다. 카메라는 장면을 분명하게 관찰하기 위해 최적의 시야각을 제공하는 위치뿐만 아니라, 잠재적인 공격자가 손 댈 수 없는 위치에 설치되어야 합니다.

3

분명한 역할 및 오너십을 정의하십시오.

많은 조직에서, 네트워크 보안 실패는 단지 어떤 직원이 특정 액세스 권한을 갖는지를 설정한 분명한 규칙과 절차가 없는 것 때문에 발생합니다.

예를 들어, 모범 사례를 따르도록 감시 시스템에 대한 보안 조치를 검토할 책임이 있는 사람이 분명하지 않을 수 있습니다. 조직에서는 "최소 권한 계정"의 원리를 사용하는 것이 좋습니다. "최소 권한 계정"이란 사용자에게 해당 작업을 수행하기 위해 필요한 리소스에 대해서만 제한된 권한을 부여한다는 의미입니다,

노출을 줄이기 위해, 영상에 액세스하는 장치는 솔루션에서 필요로 하지 않는 한 카메라에 직접 액세스할 수 없어야 합니다. 클라이언트는 VMS(영상 관리 시스템) 또는 미디어 프록시를 통해서만 영상에 액세스해야 합니다.

4

적용 가능한 최신의 펌웨어를 사용하십시오.

워크스테이션, 서버, 카메라, 프린터 및 기타 네트워크 장치에서 발견된 운영 체제의 버그나 결함으로 인해 조직이 위험에 빠질 수 있습니다.

이러한 예로는 2014년도의 유명한 하트블리드(Heartbleed) 버그입니다. 이 버그는 OpenSSL의 보안 취약점으로 해커가 서버 개인 키 및 사용자 패스워드를 알아낼 수 있었습니다.

취약점이 일반에게 알려진 후 즉시 패치가 배포되었지만, 사용자가 해당 패치를 설치하지 않으면 장치는 계속 취약한 상태로 남아 있었습니다. 이 사례는 문서로 잘 정리된 유지보수 계획이 필요하고, 펌웨어 및 모든 보안 업데이트를 통해 네트워크 장치를 최신 상태로 유지해야 하는 이유를 보여줍니다.

많은 벤더들이 일반적인 취약점과, 특정 취약점에 대한 솔루션 또는 해결책을 설명하는 노출 보고서를 공개적으로 게시하고 있습니다. 장치가 사용 가능한 최신 펌웨어로 업데이트되었습니까?

5

위험 분석을 수행하십시오.

사이버 위협 분석은 예상 손실액과 보호에 꼭 필요한 비용을 정의합니다. 잠재적인 위협뿐만 아니라, 시스템이 공격받거나 손상될 경우 발생 가능한 손해 및 비용에 대해 분석합니다. 주요 자산을 식별하고 가장 가치있는 것을 보호하기 위한 노력의 우선순위를 지정하십시오.

스스로에게 물어보십시오.

> 무엇을 보호해야 합니까?
> 누가/무엇이 위협 및 취약점입니까?
> 자산이 손상 또는 손실된 경우 어떤 영향이 초래됩니까?
> 어떤 것이 조직에 가치가 있습니까?

위험에 처할 수 있는 자산 취약점을 고려하는 것을 잊지 마십시오. 분석 및 우선순위를 준비할 때 내부 및 외부 위협을 모두 고려하십시오.

2015년 사이버 공격의 60%가 내부자에 의해 이루어졌으며, 이 중 44.5%가 "악의적"으로 간주됩니다.*

* IBM "2016 Cyber Security Intelligence Index"

6

시스템 보호 및 가능한 위협에 대한 지식을 확보하십시오.

위험 분석에 이어, 귀사의 네트워크에서 실행되는 정확한 시스템을 자세히 살펴보십시오. 선택한 장치를 사용할 때 네트워크에 발생할 수 있는 모든 위협을 이해하기 위해, 벤더의 전체 공급망과 긴밀히 협력하십시오.

이제 많은 IT 벤더가 고객 네트워크 내 자사 장치의 보안 강화에 대한 문서화된 모범 사례 또는 가이드를 제공합니다. 선택한 벤더가 이 정보를 제공하지 않는 경우, 대화를 시작하거나 다른 사용자 생성 설명서를 찾는 것이 중요합니다.

제대로 통합된 시스템에서 장치는 상호 작용해야 하기 때문에, 각 개별 장치가 아닌 시스템 전체를 이해해야 합니다. 모든 장치는 함께 작업하도록 구성될 때 그리고 자체적으로도 귀사의 IT 정책에 부합하는 것이 이상적입니다.

7

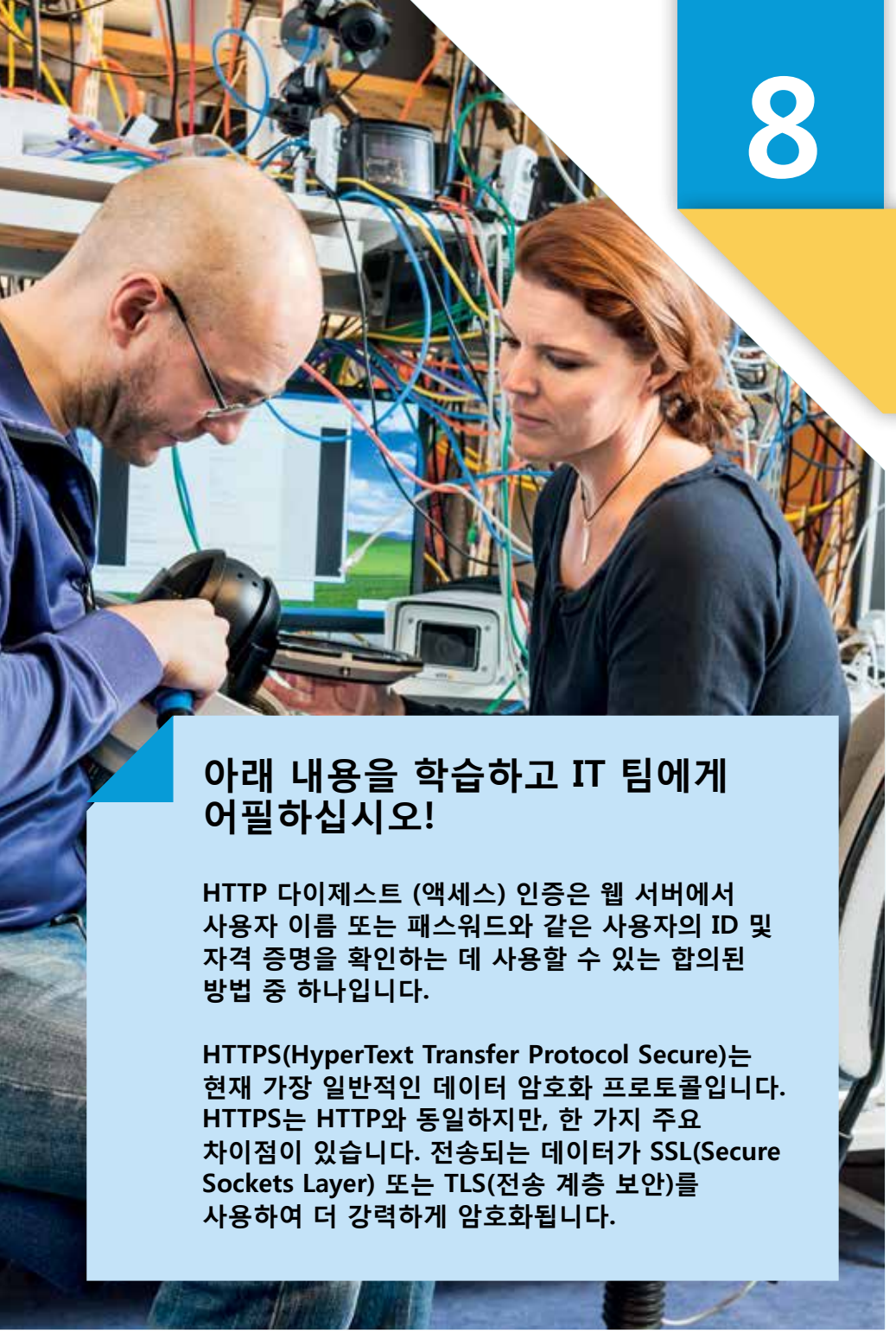
장치의 공장 출하 시 기본 설정을 변경하십시오.

장치의 기본 설정, 특히 패스워드에 의존하지 마십시오. 이러한 사항은 가장 먼저 변경해야 할 사항이며, 시스템을 보호하기 위해 수행할 수 있는 가장 중요한 단계 중 하나입니다.* 즉, 패스워드는 전체 네트워크에 대한 게이트웨이입니다.

가장 일반적인 장치에 대한 기본 어드민 계정 ID 및 패스워드는 간단한 Google 검색으로 쉽게 알아낼 수 있습니다. 공장 출하 시 기본 설정을 유지하면 해커가 더 쉽게 침입할 수 있습니다. 장치 보호 서비스를 활성화하여 구성하고, 사용하지 않는 서비스는 항상 비활성화하십시오.

시연 목적일 경우에만 기본 설정을 사용하십시오. 아무리 작은 규모의 시스템도 기본 설정에 의존할 경우 취약하게 됩니다.

* 네, #1에서 이미 말했지만 중요한 사항입니다!



8

암호화된 연결을 사용하십시오.

암호화된 연결은 로컬 또는 '내부' 네트워크를 비롯하여 모든 네트워크에 사용되어야 합니다.

귀사의 시스템에서 일반적인 인증 프로토콜인 HTTP 다이제스트 인증 및 HTTPS를 최소 하나 이상 사용하십시오. 이렇게 하면 모든 정보가 네트워크를 통해 전송되기 전에 암호화됩니다. 이러한 프로토콜을 사용하면, 악의적인 코드가 암호화되지 않은 전송을 수신하는 도청 유형의 공격 기회를 효과적으로 줄일 수 있습니다. 재무 데이터를 보호하지 않을지라도, 귀사의 데이터는 암호화를 통해 보호할 만큼 중요합니다.

아래 내용을 학습하고 IT 팀에게 어필하십시오!

HTTP 다이제스트 (액세스) 인증은 웹 서버에서 사용자 이름 또는 패스워드와 같은 사용자의 ID 및 자격 증명을 확인하는 데 사용할 수 있는 합의된 방법 중 하나입니다.

HTTPS(HyperText Transfer Protocol Secure)는 현재 가장 일반적인 데이터 암호화 프로토콜입니다. HTTPS는 HTTP와 동일하지만, 한 가지 주요 차이점이 있습니다. 전송되는 데이터가 SSL(Secure Sockets Layer) 또는 TLS(전송 계층 보안)를 사용하여 더 강력하게 암호화됩니다.

9

네트워크를 보호하십시오.

네트워크 보안이 침해되는 경우, 민감한 정보에 대한 스누핑 위험과 개별 서버 및 네트워크 장치에 대한 공격이 증가합니다.

귀사의 방화벽 및 필터를 이해하십시오. 시간을 들여 백본으로부터 네트워크를 보호하면 사이버 보안 모범 사례를 구현하려는 다른 모든 노력을 지원할 수 있습니다.

시스템의 선택에서부터 구현 및 유지관리까지, 전체 프로세스에서 IT 팀과 함께 작업하십시오.

10

시스템 및 프로세스를 유지관리하십시오.

시스템을 잘 유지관리하는 것은 가장 어려운 일 중 하나이지만, 전체 시스템을 안전하게 유지하는 데 매우 중요합니다.

정기적으로 모든 장치를 모니터링하고 적용가능하거나 지원되는 경우 시스템 알림을 활성화하십시오. 무단 액세스 시도를 감지하기 위해 액세스 로그도 정기적으로 확인해야 합니다.

일단 계획이 실행되면, 정기적으로 검토하고 평가해야 합니다. 빠르게 변화하는 기술 분야에서는 새로운 업데이트, 기능 및 모범 사례가 항상 만들어집니다. 현재 및 미래의 동료들이 프로세스를 이해할 수 있도록 유지관리 절차를 문서화하십시오.

영상 감시 및 사이버 보안의 현실

"Axis Communications가 내 사이버 보안에 관심을 갖는 이유는 무엇일까?" 라고 스스로에게 물어본 적이 있을 것입니다. 감시 영상은 귀중한 데이터 자산이며, 다른 민감한 데이터와 같이 여러 비도덕적인 목적으로 영상을 사용할 수 있는 것이 현실입니다. 범죄자는 훔친 영상을 관찰하여 고위험 자산 영역을 식별하거나, VIP 패턴을 따르거나, 카메라 사보타주를 통해 작동을 방해하는 데 사용할 수도 있습니다. 영상 서비스 거부 공격, 탬퍼링 및 훼손은 다른 잠재적 위협입니다.

IP 감시 시스템은 근거리 통신망에 위치하며 모든 IT 정책 내에서 고려되어야 합니다. 그리고 IP 카메라는 다른 네트워크 장치, 클라이언트 및 서버와 같이 보호되어야 합니다.

위협은 시스템 수준에서 관리되어야 합니다. 조직의 사이버 보안은 귀하만의 관심사가 아닙니다. 네트워크, 해당 장치 및 서비스를 보호할 책임은 전체 벤더 공급망에 있습니다. 이와 함께 인력, 프로세스 및 기술을 고려해야 합니다.

네트워크 보안 위반의 대다수는 인적 오류, 과실, 잘못된 구성 및 유지보수 불량으로 인해 발생합니다. IT 네트워크 보안 정책이 감시 네트워크에 항상 적용되는 것은 아니지만, 해당 정책 내에서 고려해야 할 사항입니다.

선택할 수 있는 힘은 귀하에게 있습니다. 기존 네트워크 보호를 저하시키지 않으면서 보호된 영상 시스템을 설치하는 방법을 권장하는 영상 감시 제조사를 선택하십시오. IT 팀 및 솔루션 제공업체와 함께 작업하여 위험 분석, 시스템 개발 및 유지보수를 처리하십시오.

사이버 보안을 위한 회사 문화 구축

열악한 사이버 보안 상태가 빈번해지면 조직을 괴롭힙니다. 이러한 일이 귀하에게 발생하지 않도록 하십시오! 사이버 보안 사례에 대한 직원의 지식이 증가하면 보안 위험이 30% 감소한다고 보고되었습니다.*

사이버 보안 동맹을 형성하십시오. 조직 내에 IT 정책을 알고 있는 사람은 많을 수록 좋습니다. 사이버 보안 팀 외부에 있는 개인도 해당 정책에 동의하고 준수할 뿐만 아니라, 이 정책을 완전히 이해해야 합니다.

보너스 모범 사례!

보안 네트워크를 생성하고 유지관리하는 것은 팀 전체의 노력이며 다른 여러 부서의 지원이 필요합니다. 혼자서는 이를 수행할 수 없습니다.
계획이 마련되면, 조직 전체에 공유하고 새 장치를 선택하여 네트워크에 설치할 때 해당 계획을 가장 우선적으로 고려하십시오

사이버 보안을 위한 문화를 어떻게 구축하고 유지할 수 있을까요? 해결 방안을 개발할 때 다음 사항을 고려하십시오.

> 직원 보안 상태 교육에 투자
> 신규 직원 입사 시 프로세스에 대해 교육
> 고위 간부가 사이버 보안의 중요성을 알리도록 격려
> 진화하는 사이버 위협이 나타날 때, 이에 대해 지속적으로 학습하고 알려진 위협에 대해 조직의 적절한 구성원과 공유
> 새로운 네트워크 장비를 선택할 때 사이버 보안을 필수 요건으로 검토
> BYOD(Bring Your Own Device) 정책 구현
> 사이버 보안 사고 대응 전략을 수립하고 침해 발생 시 적용

사이버 보안 계획에 대한 조직 전체의 동참을 구하면, 네트워크 및 장치의 보안을 유지하는 것이 훨씬 용이해집니다.

* 2015 Global Megatrends in Cybersecurity(Rep.). (2015). Ponemon Institute LLC. Ponemon Institute© 수행.

결론 및 추가 리소스

사이버 보안 위협이 증가 및 진화하고 있습니다. 따라서 네트워크 보안 상태에 대해 사전 예방적으로 대응하는 것이 이전보다 더 중요하게 되었습니다. 위험을 완화하고 침해 시 이에 대응하는 방법에 대한 계획을 수립하면, 귀하의 조직은 현재 취약점을 완화하고 향후 잠재적 해킹을 방지할 수 있습니다.

데이터 및 네트워크 보호 전략을 따르면, 침해가 발생하기 어렵고 침해를 위한 시간과 리소스 모두 많이 소요되도록 만들 수 있습니다.

성공을 위한 다음 핵심 요소를 기억하십시오.

- 감시 네트워크를 포함하여 모든 네트워크에서 IT 정책을 구현
- 전체 공급망에 관여
- 사용자 교육을 우선시
- 사이버 보안을 회사의 문화로 수용
- 사용하기 쉬운 프로세스를 정의
- 올바른 시스템 구성, 업데이트 및 모니터링을 실시
- 사용 가능한 리소스를 활용하고 실행

사이버 보안은 무서운 것이 아닙니다. 대부분의 공격은 성공하지 못한다는 점을 명심하십시오. 성공하지 못한 사례를 듣지 못한 것뿐입니다. 귀하가 데이터 및 네트워크를 보호하기 위해 적절한 조치를 취하는 한, 귀하는 사이버 보안을 향상하고 침해의 위험을 완화하기 위해 노력하고 있는 것입니다.

자, 그럼 귀사의 네트워크, 그리고 네트워크 상에서 운영되고 있는 장치들이 얼마나 안전한가요?

보다 자세한 정보를 보시려면, 다음 웹사이트를 방문하시기 바랍니다:

www.axis.com/kr/ko/about-axis/cybersecurity

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