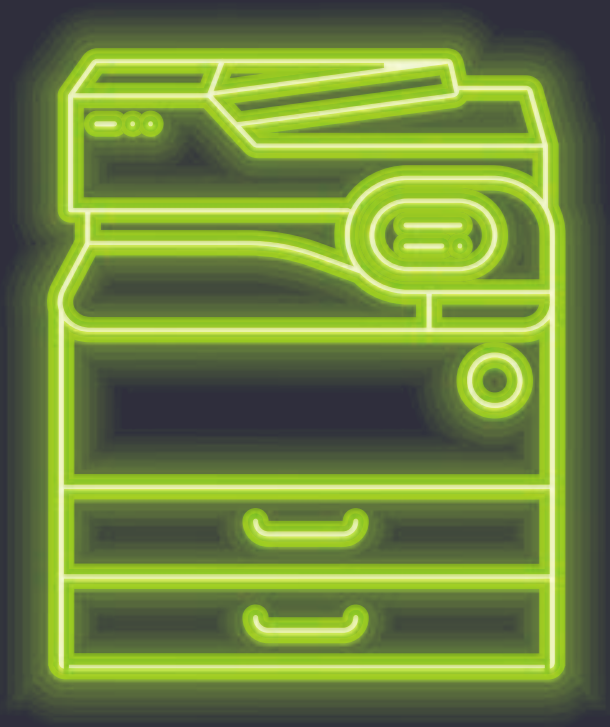
프린터 보안: 새로운 IT 필수 요소

연구 결과, '프린터'는 보안 사각 지대



목차

소개

IT 보안 위협이 갈수록 증가하고 있는 반면, 하드웨어 보안을 위한 노력은 그에 미치지 못하고 있습니다. 이러한 추세는 무엇보다 프린터 사용에서 두드러집니다. IT 전문가들 사이에서는 비보호 프린터가 네트워크에 미치는 위험에 대해 점점 더 인식이 높아지고 있지만, 여전히 프린터는 보안 사각지대에 놓여 있으며, 대다수는 보호되지 못하고 있습니다.

"험블 네트워크 프린터를 포함해, 네트워크에 연결된 모든 종류의 기기가 취약성에 노출되어 있다"라고 HP 남태평양 프린팅 시스템 디렉터 Ben Vivoda는 지적합니다. "프린터가 관심을 받지 못하고 삭제 위험에 노출되는 것을 흔히 볼 수 있습니다. 이제 기업들은 전반적인 IT 사이버 보안 전략에서 더 이상 프린터를 간과할 수 없습니다."[1]

설문을 진행한 Spiceworks사에 따르면, 실제로 프린터는 갈수록 증가하는 다양한 보안 위협의 원인이 되고 있습니다. 오늘날 프린터는 2016년에 비해 외부 위협이나 침해의 원인이 될 가능성이 68% 높아졌으며, 내부 위협이나 침해의 원인이 될 가능성은 118%나 증가했습니다.

그러나 프린터가 초래하는 보안 위험을 인지하는 IT 전문가는 겨우 30%에 불과합니다. 이러한 수치는 2016년에 비해 약 두 배로 증가하기는 했으나, 여전히 낮은 수치로 위험한 현실을 반영합니다. 다수의 IT 전문가들은 프린터 보안에 대한 구시대적인 관점을 유지하고 있으며, 네트워크 내부에서 사용하는 프린터는 안전하다는 낡은 인식에서 벗어나지 못한 것으로 보입니다.

심지어 이러한 위험을 인식하고 있는 IT 전문가들조차, 넘쳐나는 엔드 유저 기기의 보안을 최우선 순위로 보고 프린터와 네트워크의 보안은 간과합니다.[2] 과거에는 프린터 보안이 다른 엔드포인트에 우선 순위를 내주는 것이 가능했지만, 이제는 보안되지 않은 프린터가 광범위한 IT 인프라와 전반적인 기업 리스크 거버넌스에 미치는 위험을 해결하는 것이 IT 기업의 필수 과제가 되었습니다.

비즈니스에 초래하는 위험

정말로 프린터가 문제인가요? 한마디로 말하자면, 그렇습니다. 새로운 보안 위협이 매시간 발생하는 시대에, 프린터는 쉬운 공격 대상이 될 수 있습니다. "최신 프린터는 근본적으로 고급 네트워크 호스트이며, 따라서 기존의 컴퓨터에 상응하는 보안 노력이 요구됩니다." Kevin Pickhardt가 월간 Entrepreneur 칼럼을 통해 지적한 내용입니다.[2] "오피스 프린터는 데이터 손실 및 기밀정보 유출의 근원뿐만 아니라 해커들이 악용하는 공격 벡터도 될 수 있습니다." 관련 사례로, 지난해 한 해커가 자동화된 스크립트를 이용하여 다량의 영수증 프린터를 포함한 공개 접속 가능 프린터 150,000대에 접속하여 불법 인쇄 작업을 수행한 사건이 보도된 바 있습니다.[3]

업계 분석가들도 이에 동의하고 있습니다. IDC사에 따르면, "대부분의 프린터가 내부 네트워크에 광범위한 접근 권한을 가집니다. 해커는 프린터 한 대만 접수해도 기업 전체의 네트워크, 애플리케이션 및 데이터 자산에 무제한으로 접근할 수 있게 됩니다."[4]

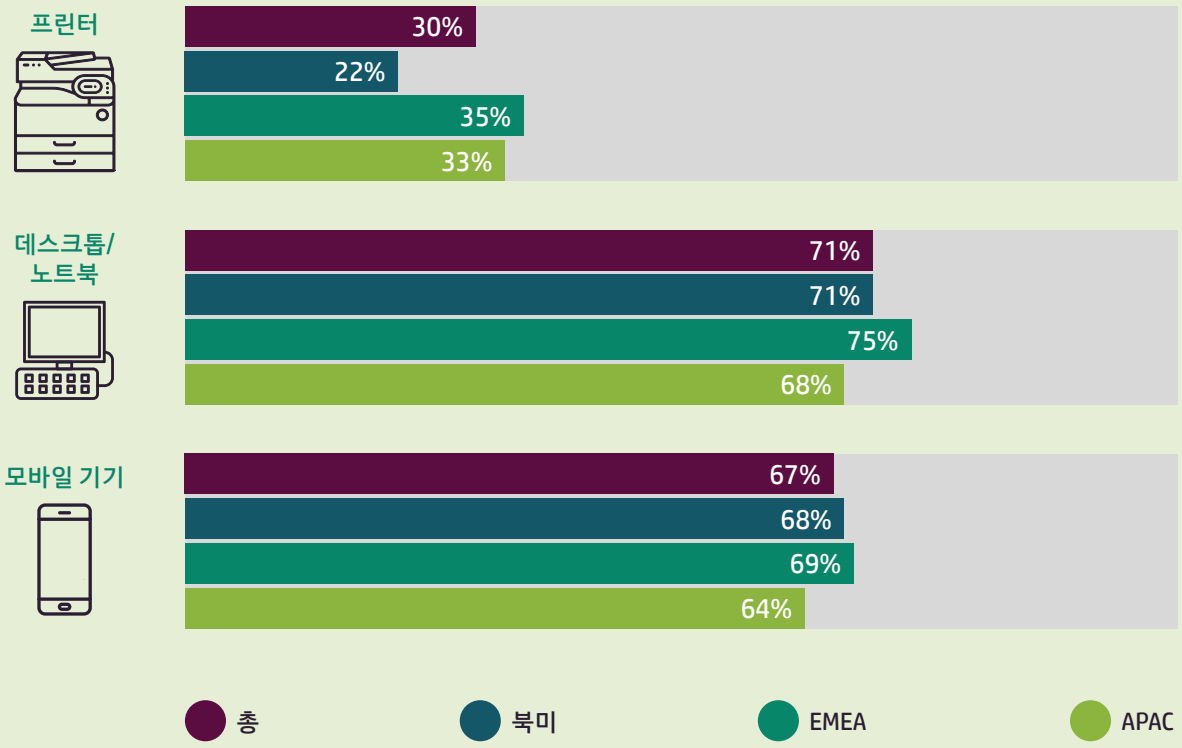
보안이 취약한 네트워크 프린터란 어떤 상태인가요? 접속에 큰 제약이 없으며 광범위한 네트워크 프로토콜에 무방비로 노출되어 방치된 상태입니다. 접근 제어(심지어 관리자 비밀번호 설정도 흔히 간과됨)를 요구하지 않습니다. 보안에 민감한 서류가 인증 없이도 인쇄되어 프린터의 출력 용지함에 하루종일 방치될 수 있으며, 네트워크상에서 암호화되지 않은 데이터를 전송합니다. 오래된 펌웨어를 실행하거나 보안 위협에 대한 모니터링이 이루어지지 않습니다.

이와 같이 미흡한 보안 기능은 심각한 결과를 가져오게 됩니다. 리서치 기관 Gartner는 2020년까지 사물인터넷(IoT) 프로젝트의 절반 이상이 하드웨어 보안 구축에 실패함으로써 보안에 민감한 정보를 유출하게 될 것으로 예측하고 있으며, 이는 오늘날의 5% 미만에서 크게 증가한 수치입니다.[4]

인식의 문제

이러한 연구 결과에도 불구하고, IT 전문가들은 여전히 프린터가 초래하는 위험을 제대로 인지하지 못하고 있습니다. 북미에서는 프린터를 보안 위험으로 인식하는 IT 전문가가 4분의 1도 되지 않으며(22%), 유럽과 중동 및 아프리카(EMEA)에서도 3분의 1을 겨우 웃도는 수준인 35%에 불과합니다.

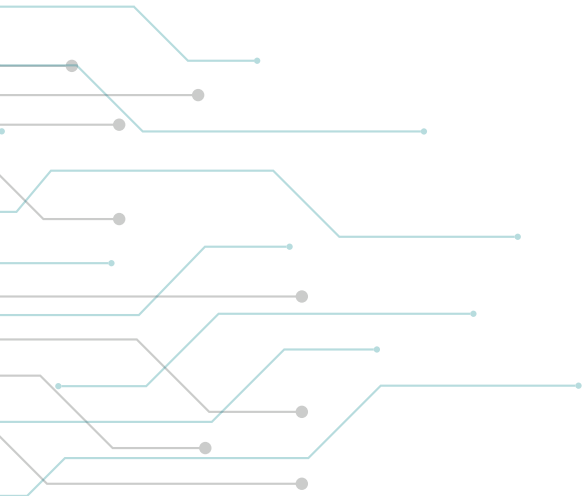
보안 위험의 인식 수준



그에 반해 IT 전문가들은 데스크톱과 노트북이 초래하는 위협을 71%, 모바일 기기가 초래하는 위협을 67%로 평가했습니다.

더 나아가 Spiceworks사의 연구 결과는 예방 조치를 취하는 IT 전문가들이 매우 부차적인 접근을 취하고 있음을 보여줍니다. 보안 요건이 매우 포괄적임을 감안할 때, 이는 놀라운 현상은 아닙니다. 만능의 단일한 솔루션은 없습니다. 예를 들어 방화벽 하나로는 충분하지 않습니다. 모든 네트워크 기기와 같이, 프린터 보안은 여러 각도에서 접근해야 합니다. 그리고 모든 보안 전략과 마찬가지로, 다수의 효과적인 솔루션이 통합되고 자동화되어야 하며, 사용 및 관리가 용이해야 합니다.

이러한 도전 과제가 더욱 어려운 이유는 프린터 브랜드마다 각자 다른 특허 소프트웨어와 운영 시스템을 사용하기 때문입니다. 많은 IT 전문가들이 기업의 보안 정책을 만족하는 프린터 소프트웨어를 구성할 만큼 충분한 지식을 갖추지 않았을 수 있습니다.



최근 관행

IT 전문가들은 현재 보유하고 있는 도구와 그러한 도구에 대한 지식을 바탕으로 하여 보안 정책 및 기능을 맞춤형으로 개발함으로써 다양한 방식으로 프린터 보안에 접근하고 있습니다. 그러나 프린터 보안을 위한 최근 관행은 대략 여섯 가지에 국한됩니다.

프린터 보안을 위해 해당 보안 조치를 실시하고 있는 응답자의 비율


42% 서류 보안


31% 기기 보안

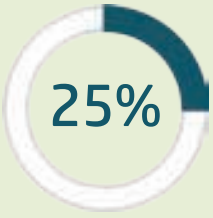

40% 네트워크 보안


30% 보안 모니터링

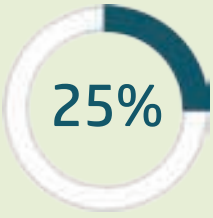

39% 접근 제어


28% 데이터 보호

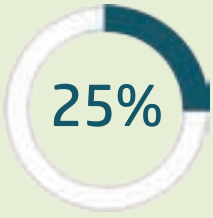
연구 결과에 따르면 IT 전문가들은 이러한 카테고리 내에서 다양한 기본 보안 조치를 실시하고 있지만, 매우 낮은 비율에 그칩니다.



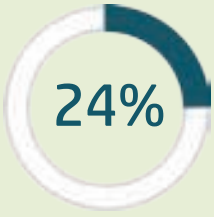
사용하지 않는 열린 포트 닫기



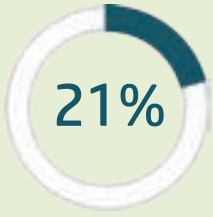
'발송처' 표시 기능 활성화하기



프린터 수리에 보안 접속 적용하기



개인정보 보안 ('Pull') 프린팅 구현하기

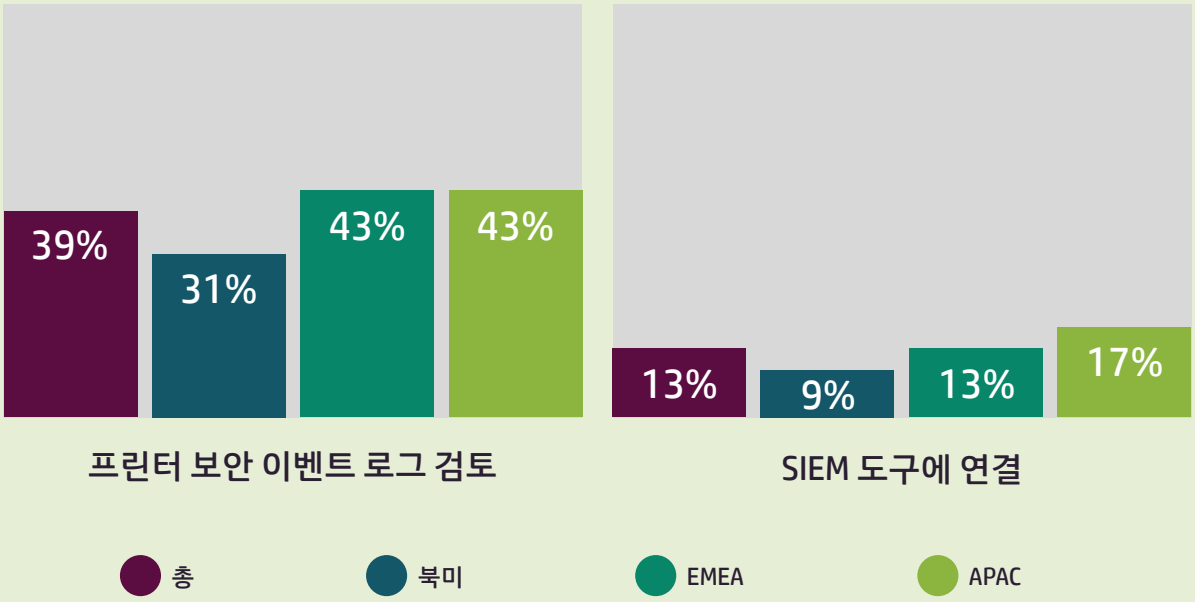


프린터 하드 드라이버 삭제를 습관화하기

정기적으로 작업을 종료하거나 삭제하고, 구성 변경을 위해 관리자 접근 권한을 요구하거나 인증서 관리를 자동화하는 IT 전문가는 더욱 드뭅니다.

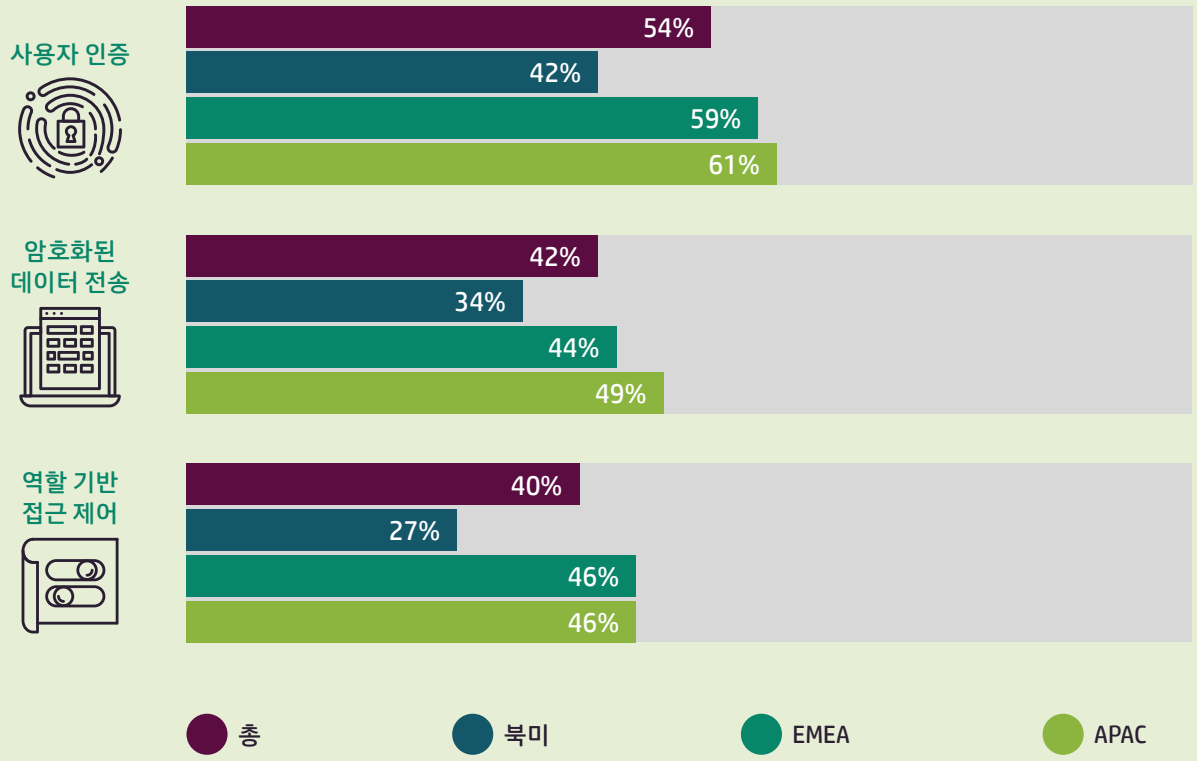
IT 전문가들은 프린터 보안 모니터링을 다른 작업보다 빈번하게 수행하고 있으나, 그 비율은 여전히 낮은 편입니다. 프린터 로그를 정기적으로 검토한다고 응답한 IT 전문가는 겨우 39%였으며, 북미의 경우에는 31%에 불과합니다. 프린터를 SIEM 도구에 연결하는 경우, 이러한 비율이 13%에 그쳤습니다. 프린터 로그를 모니터링하지 않고 프린터를 SIEM에 통합하지 않으면 IT 전문가는 모니터링되지 않는 인프라를 통해 네트워크에 숨어들어 데이터를 유출하는 사이버 범죄를 인지하기가 어렵습니다.

프린터 모니터링



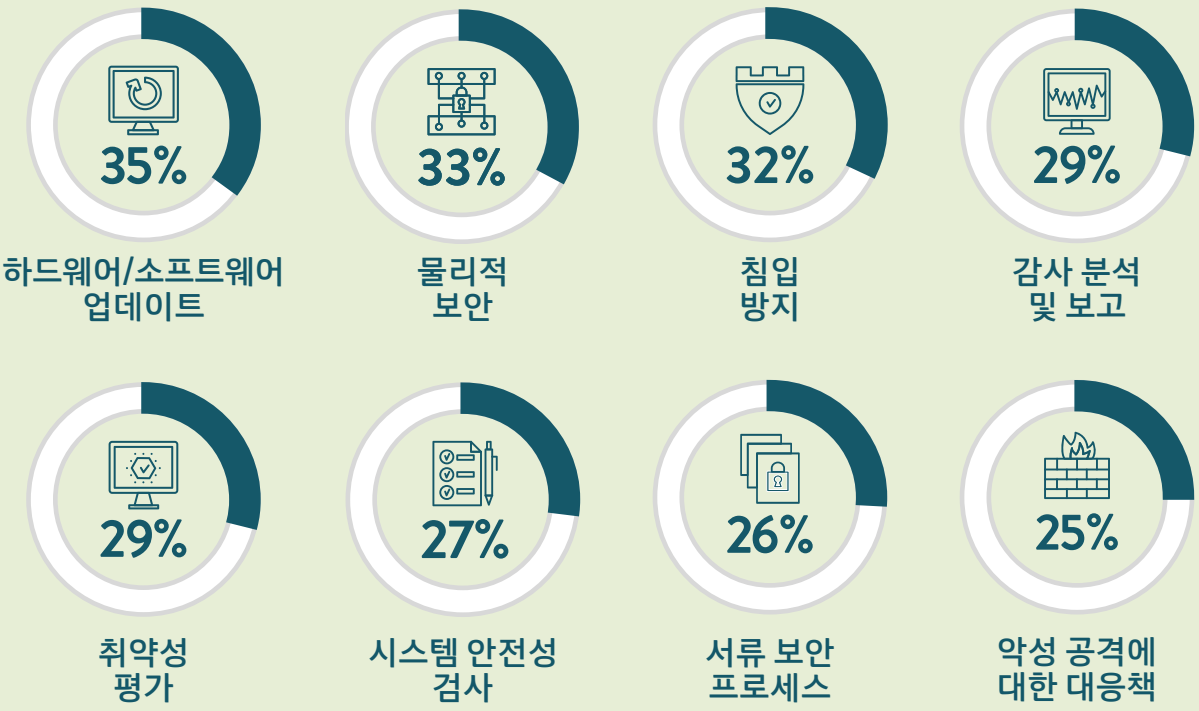
연구 결과는 프린터 보안에 있어 지역적 차이가 있으며, 이 가운데 북미 지역이 뒤쳐져 있음을 보여줍니다. 이런 현상은 특히 접근 제어와 암호화에서 더욱 두드러집니다. APAC 지역의 IT 전문가들은 암호화된 데이터 전송, 기기 인증 요구, 사용자 역할에 따른 접근 제어를 실행함에 있어 북미 지역의 전문가들보다 훨씬 앞서 있습니다.

현재 도입된 프린터 보안 관행



마지막으로 데이터 개인정보 규제의 준수에 있어 IT 전문가들은 다중적인 접근 전략을 취하고 있으며, 일부 프린터 제어 전략이 전반적인 IT 컴플라이언스 전략에 포함되어 있습니다. Spiceworks사는 설문 조사에서 IT 전문가들이 미국 인터넷 보안 센터(CIS)의 'CIS Controls V7'에 근거해 어떤 컴플라이언스 제어를 구축했는지를 질문했습니다.[5]

사용 중인 컴플라이언스 제어



본 데이터는 IT 전문가들이 종종 펌웨어 업데이트와 같은 가장 기본적인 프린터 보안 조치를 간과하고 있으며, 이러한 조치를 컴플라이언스 관행의 일부로 정착시킨 경우는 3분의 1에 불과함을 보여줍니다. 업계의 연구 결과도 일치합니다. IDC사에 따르면, 흔히 프린터 펌웨어는 최신 버전으로 업그레이드되어 있지 않으며 이는 종종 기업들이 위험을 과소평가하기 때문입니다.[4] 또한 조직 전반에 걸쳐 프린터의 새로운 펌웨어를 검토하고 테스트하여 도입할 시간이 충분하지 않습니다.

포괄적인 프린터 보안을 위해

보안 대책을 실시하고 있다고 응답한 84%의 IT 전문가 가운데, 프린터를 보안 대책에 포함시킨 응답자는 64%에 불과합니다. 북미의 경우에는 겨우 52%에 그쳤습니다. 통합되고 자동화된 프린터 보안 통제를 추구하고 이를 실제로 구현해야 하는 이유가 바로 여기에 있습니다. 빌트인 보안 기능을 탑재한 프린터는 귀사의 위험을 최소화하는 동시에 귀하의 IT 투자 효과를 극대화합니다.

IDC사의 분석은 또한 다음과 같은 사실을 발견했습니다. “프린터는 완성품의 경우 보안 기능을 강화하기가 매우 까다로우며, 이는 기본적으로 높은 수준의 보안 기능을 충분히 갖춘 프린터를 선택하는 것이 중요함을 의미합니다.”[4] Gartner사는 다음과 같이 지적합니다. "신흥 프린팅 시장의 역동성을 활용하기 위해 기술 전략 기획자들은 보안 업계의 모범 관행을 넘어서는 단계의 솔루션 패키지를 사용하여 포괄적인 프린팅 보안 솔루션 포트폴리오를 구축해야 합니다. 이러한 솔루션을 보다 광범위한 보안 솔루션 에코시스템에 통합해야 합니다."[6]

관리형 프린팅 서비스 공급자들은 프린터 보안을 다루는 데 필요한 지식을 갖춘 직원군을 보유하지 못한 IT 부서를 지원하기 위해 서비스를 확대하고 있습니다. IDC사는 다음과 같이 설명합니다. “공급자들은 기기 및 데이터 수준의 보호 서비스를 다양하게 제공하며, 이들 중 상당수가 기존 서류 관리와 문서 보완(ECM) 시스템을 통합하여 보다 높은 수준의 보안을 제공하고 거버넌스 및 규제 준수 문제를 다루도록 설계되었습니다.”[7]

IT 전문가들에게 있어 다행스러운 점은, 오늘날 첨단 프린터는 기업의 프린팅 보안 포트폴리오를 위해 위협 감지, 보호, 알림 및 자가 치료 등 다양한 보안 기능을 탑재하고 있다는 것입니다. 이로 인해 귀사의 네트워크에서 가장 취약한 엔드포인트인 험블 프린터의 보안을 강화하기가 어느 때보다도 용이해졌습니다.

귀사의 프린터 보안을 강화할 때입니다.

자세히 보기

설문 개요

HP는 2018년 5월 Spiceworks사에 설문 조사를 의뢰했습니다. 본 설문은 IT 디렉터, IT 매니저 및 기타 IT 담당자를 포함한 IT 의사결정권자를 대상으로 최근의 프린터 보안 관행을 파악하고 위험 요인을 규명하고자 실시되었습니다. 설문 결과는 북미, EMEA 및 APAC 지역에서 직원 250명 이상 규모의 회사에 근무하는 응답자 약 500명의 응답을 포함합니다.

자료 출처

1 McLean, Asha, "Unsecured printers a security weak point for many organisations: HP," ZDNet (2017년 4월 18일) https://www.zdnet.com/article/unsecured-printers-a-security-weak-point-for-many-organisations-hp/

2 Pickhardt, Kevin, "Why Your Innocent Office Printer May Be a Target For Hackers," Entrepreneur (2018년 1월 31일) https://www.entrepreneur.com/article/308273

3 Peyser, Eve, "Hacker Claims He Hacked 150,000 Printers to 'Raise Awareness' About Hacking," Gizmodo (2017년 2월 6일) https://gizmodo.com/hacker-claims-he-hacked-150-000-printers-to-raise-aware-1792067012

4 Brown, Duncan, et al., "IDC Government Procurement Device Security Index 2018," IDC (2018년 5월)

5 "CIS Controls," Center for Internet Security (2018년 3월) https://www.cisecurity.org/controls/

6 Von Manowski, Kristin Merry and Deborah Kish, "Market Insight: IoT Security Gaps Highlight Emerging Print Market Opportunities," Gartner (2017년 10월 31일) https://www.gartner.com/doc/reprints?id=1-4OCKFKG&ct=180110&st=sb

7 Palmer, Robert and Allison Correia, "IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment," IDC (2017년)