백서

아무도 지키지 않는 문

많은 프린터가 사이버 공격에 취약하다는 연구 발표

IT 팀이 다른 엔드포인트의 보안에 집중하는 사이 회사의 프린터 보안은 무방비로 방치되었습니다.

프린터는 손쉬운 먹잇감: 네트워크에 연결된 수많은 프린터는 아무런 제한이 없고 안전하게 보호되지 않습니다.

그러나, 위협은 항상 존재하고 이를 간과해서는 안 됩니다. 기업용 프린터는 네트워크에 연결된 다른 엔드포인트와 동일한 약점을 지닌 강력한 네트워크 장치로 진화했습니다. 이렇게 보안되지 않은 진입점은 사이버 공격에 쉽게 노출될 뿐만 아니라 외부에서 회사의 재무 및 개인적인 데이터에도 쉽게 접근할 수 있게 하기 때문에 매우 심각한 문제를 초래합니다.

그럼에도 불구하고, 300명 이상의 기업 IT 의사결정권자들을 대상으로 실시한 최근 설문조사에서는 응답자의 16%만이 프린터가 보안 위협에 매우 취약하다고 답변하여 데스크톱/노트북, 모바일 장치에 비해 현저히 낮았습니다.[1] 이러한 인식은 IT 직원이 네트워크 보안을 대하는 자세에도 악영향을 미쳤습니다. 5개 기업 중 3군데 정도의 기업만이 프린터 보안에 대한 대책을 수립하였으며, 이는 다른 엔드포인트에 비해 현저히 낮은 수치입니다. 또한, 프린터를 보호할 수 있는 간단한 솔루션이 있음에도 프린터를 취약한 상태로 방치해 두고 있었습니다.

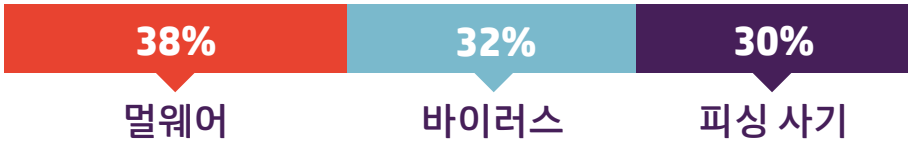
본 백서는 Spiceworks 설문조사, 보안 위협의 영향, 사이버 공격에 대비한 최근 프린터들의 일부 기능 등 프린터 보안에 대한 데이터가 포함되어 있습니다.

불과 16%의 응답자만이 프린터가
보안 위협에 취약하다고 생각합니다.[1]

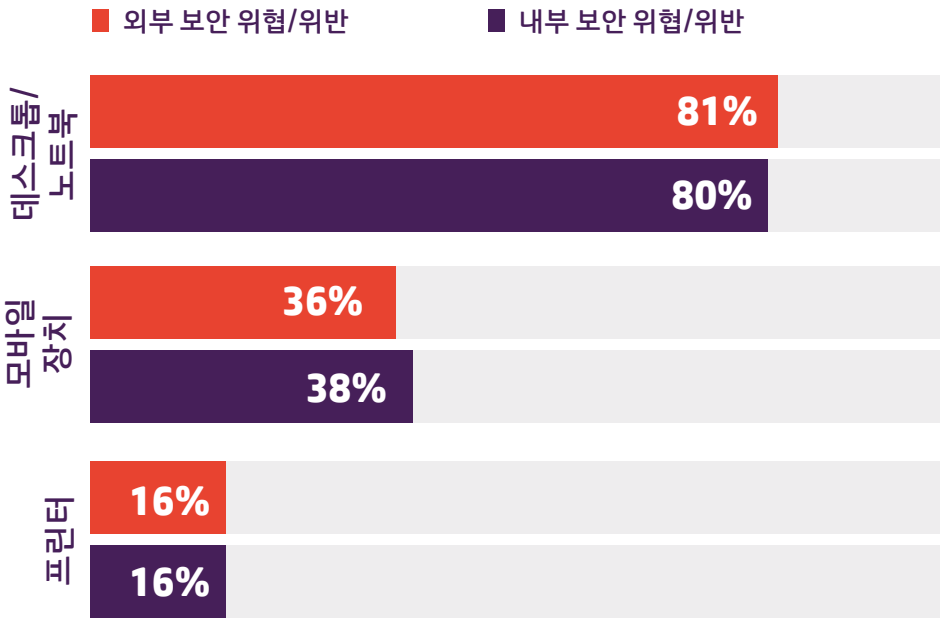
공격의 진입로

Spiceworks 설문조사에 따르면 순수 응답자의 74%가 작년에 회사에서 최소한 몇 번의 외부 IT 보안 위협이나 위반 사례를 경험했다고 답변했습니다. 그리고, (순수) 응답자의 70%가 내부 IT 보안 위협이나 위반 사례를 경험했으며, 사용자의 실수, 개인 장치를 업무용으로 사용, 가정 또는 공용 네트워크에서 업무를 수행한 사례가 주를 이루었습니다.[1]

외부 IT 보안 위협/위반의 주요 사례



데스크톱 및 노트북을 통한 위협이 가장 많았으며, 그 외에는 모바일 장치와 프린터였습니다.[1] (16%가 프린터를 통해 침입했다는 수치는 2014년 Spiceworks 설문조사의 4%에 비해 급격히 증가했습니다.) 하지만, 프린터는 PC와 모바일 장치만큼 세세히 모니터링되지 않기 때문에 프린터를 통한 공격 횟수가 과소평가되었을 수 있습니다.



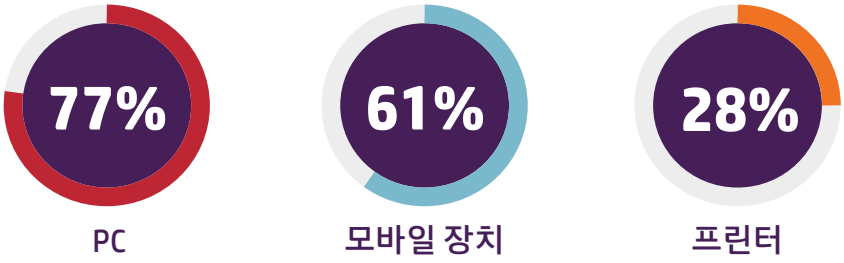
방치되는 프린터

어떤 사례이든 간에, Spiceworks의 설문조사는 프린터 보안이 항상 뒷전이 됨을 명확히 보여줍니다.

대다수의 기업들은 네트워크, 엔드포인트, 데이터 보안의 중요성을 명확히 인식하고 있습니다. 실제로, 응답자의 3/4 이상이 네트워크 보안, 액세스 제어/관리, 데이터 보호, 연결 장치 보안을 적용 중이거나 이들을 복수조합하여 적용하고 있습니다.[1]

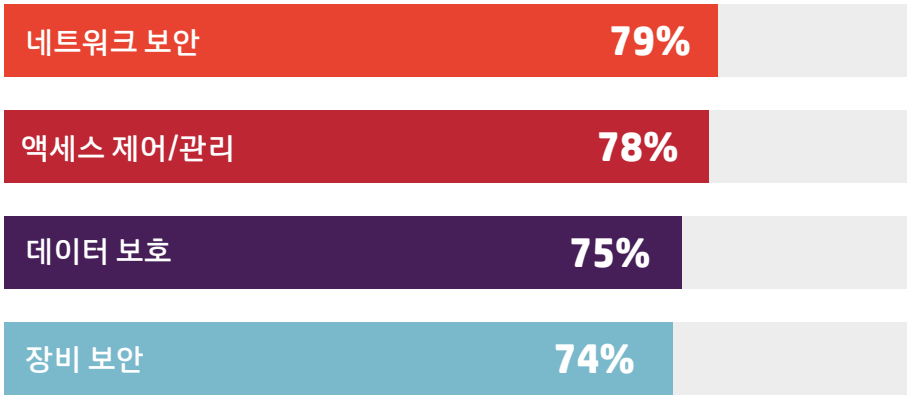
하지만, 이런 솔루션들이 프린터에 적용되는 비율은 현저히 낮습니다. 응답자의 83%가 데스크톱/노트북에, 55%가 모바일 장치에 네트워크 보안을 적용하지만 프린터에 적용 중인 비율은 불과 41% 였습니다.[1]

이러한 차이는 엔드포인트 보안에서 가장 두드러집니다.



또한, 전체 응답자의 1/3도 안 되는 응답자(28%)만이 프린터에 보안 인증서를 배포하고 있었습니다. 이에 반해 PC는 79%가, 모바일 장치는 54%가 보안 인증서를 배포하고 있습니다.[1]

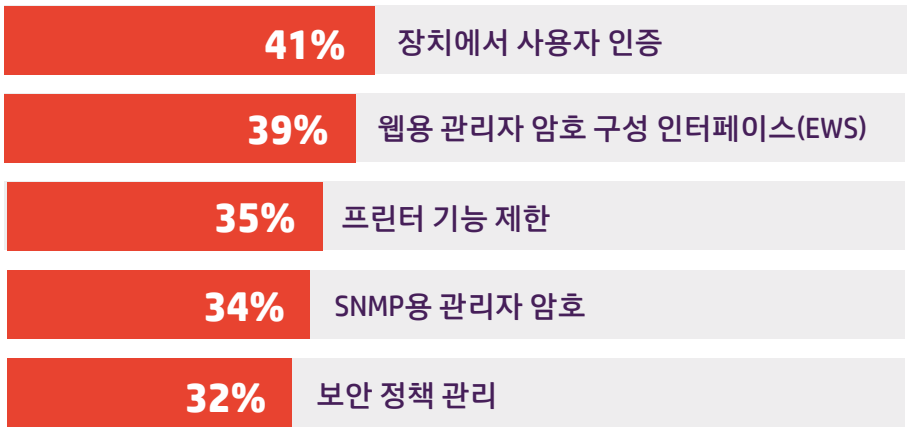
엔드포인트 보안의 주요 솔루션



일반적으로 엔드포인트 보안으로 사용되는 보안 대책 중 가장 많이 사용되는 프린터 보안 솔루션은 문서 보안, 네트워크 보안, 액세스 제어였으며, 응답자의 절반 미만이 회사에서 이런 솔루션을 프린터에 적용하고 있다고 답변했습니다.[1]

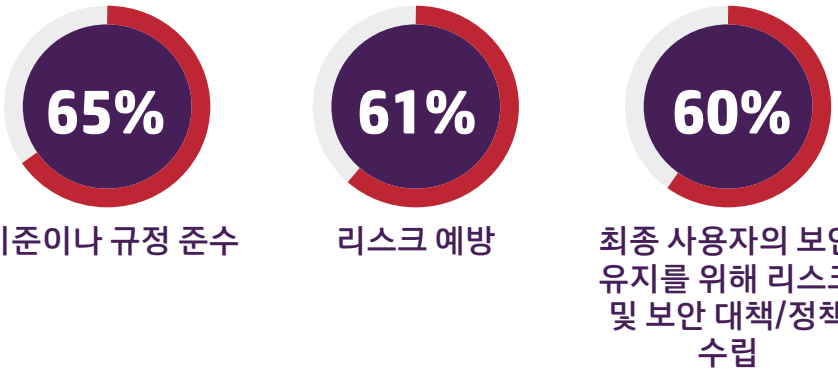
일부 기업에는 프린터만을 위한 보안 대책도 있지만, 이런 대책도 기업간의 차이가 큽니다. 40%를 겨우 넘는 기업에서 사용자 인증을, 40% 미만이 웹 구성 인터페이스에 관리자 암호를 사용하고 있습니다.[1] 강력한 보안 대책을 수립하려면 모든 기업들이 모든 대책을 함께, 그리고 더욱 많이 사용해야 합니다.

프린터 전용 주요 보안 대책



엔드포인트 규정 준수 및 감사 대책의 경우, 프린터 보안 제어가 다른 엔드포인트에 비해 소홀히 다루어지고 있습니다. 90%의 기업들이 정보 보안 정책을 가지고 있지만, 이런 정책은 대부분 프린터까지 적용되지 않습니다. 예를 들어, PC의 경우 응답자의 57%가 멀웨어 방어 대책이 구축되어 있다고 응답한 반면, 프린터의 경우는 응답자의 17%만이 대책이 구축되어 있다고 답변했습니다.[1]

90%의 IT 전문가들은 다음과 같은 이유로 자신의 회사에 정보 보안 정책이 구축되어 있다고 합니다.



이와 같이 기업들이 프린터 보안을 중요하게 생각해야 함에도 그렇게 하고있지 않은 것이 자명히 드러납니다.

HP의 수석 보안 고문인 Michael Howard 씨는 "수많은 프린터들이 여전히 기본값으로 설정된 암호를 사용하거나, 암호가 전혀 설정되지 않았거나, 동일한 암호를 사용하고 있습니다. 암호로 보호하지 않은 프린터는 해커에게는 금맥과 같습니다. 우리가 흔히 접할 수 있는 위반 사례 중 하나가 중간자 공격입니다. 해커가 프린터의 [수신 문서]를 가로채서 인쇄하기 전에 노트북으로 보내는 수법입니다. 해커들은 CEO가 인쇄하는 모든 문서도 볼 수 있습니다." 라고 말합니다.[2]

프린터 침입의 잠재적 영향

Bitdefender에서 수석 온라인 위협 분석가로 근무하는 Bogdan Botezatu 씨에 따르면, 프린터에는 매우 큰 잠재적 보안 허점이 있다고 합니다. "당사의 취약성 평가 연구실에는 수많은 원격 분석 기법이 있습니다. 라우터는 더 이상 인터넷 침입에 대한 최약체 장치가 아닙니다. 이제 프린터가 그 역할을 대신합니다."[3]

이런 취약성은 비즈니스에 막대한 영향을 미칠 수 있습니다. 한 대의 취약한 프린터로 인해 네트워크에 연결된 모든 장치들이 공격을 받을 수 있으며, 해커들이 네트워크에 연결된 장치에 스파이를 심어 놓고 전제 네트워크에 침입할 수 있습니다.

1. 헬프 데스크 통화량 및 지원 시간 증가

2. 생산성/효율성 감소

3. 시스템 가동 중단시간 증가

4. 지원 통화에 소요되는 시간 증가

5. 최종 사용자 정책의 강화

이렇게 보안 붕괴의 영향에 대해 알아봤습니다. Spiceworks 설문조사에서 응답자들이 답한 보안 붕괴의 Top5 영향이었습니다.[1]

그러나, 프린터 침입은 특히, 인쇄된 데이터를 전자적으로 저장할 수 있는 복합기를 사용할 경우에 더욱 심각한 결과를 초래할 수

있습니다. 프린터 캐시에 저장된 인쇄 작업은 해커들이 민감한 개인 정보나 기업 정보에 액세스할 수 있도록 해줍니다.

더욱 심각한 문제는 해커들이 미보안 프린터를 통해 광범위하게 회사 네트워크에 침입하여 주민등록번호, 금융 정보 또는 내부 메모와 문서 등을 훔칠 수 있다는 점입니다. 이렇게 훔친 정보는 직원 개인에게 영향을 미칠 수 있을 뿐만 아니라 경쟁업체에서 사용될 수도 있으며 회사의 명성을 심각하게 훼손시킬 수도 있습니다.

간단한 솔루션: 내장된 보안 기능

기업들은 프린터의 보안까지 신경을 써야 합니다. 오늘날의 일부 기업용 프린터는 사용이 편리하고 프린터 위협을 차단할 수 있는 보안 기능이 탑재되어 있습니다. 이 기능에는 다음의 것들이 포함되어 있습니다.

- **공격 자동 감지, 보호, 복구**
- **승인되지 않은 사용을 방지하기 위해 사용 추적**
- **PIN 또는 스마트카드 등 간단한 보안 로그인 옵션**
- **사용자가 ID 배지를 사용하여 프린터에서 빠르게 인증하고 안전하게 인쇄할 수 있는 근접 카드 판독기**
- **민감한 문서를 암호화하여 안전하게 인쇄**

추후에 데스크탑이든 복합기든 프린터를 고려할 때 통합 보안 대책을 검토하고 활성화해야 합니다. 이와 같은 간단한 프린터 내장 기능을 사용하면 프린터를 무방비 상태로 방치하지 않아도 됩니다. 다른 사물 인터넷에는 걱정할 액세스 포인트가 무궁무진하지만 프린터만큼은 걱정하지 않을 수 있습니다.

좀 더 안전한 프린터를 원하세요?
자세히 알아보기 >

출처:

1 2016년 11월 HP를 대신하여 북미, EMEA, APAC에서 309명의 IT 의사결정권자를 대상으로 실시된 Spiceworks 설문조사.

2 "프린터 보안: 여러분 회사의 데이터는 정말 안전한가요?" *Computerworld*, 2016년 6월 1일. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

3 "사물 인터넷 중 가장 취약한 프린터" *The Register*, 2016년 9월 8일. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/