VOLUME 4

디지털 및 사회적 격차 해결

SMB dynamo

The People and Cisco Technologies Propelling Small and Medium Businesses

기술 동향

전문가 관점

디지털 여정

SMB dynamo

스토리 링크

기술 동향

보안: 거세지는 사이버 공격에 맞서기 위한 중견·중소기업의 우선 과제

중견·중소기업에서 "제로 트러스트" 보안을 도입해야 하는 이유

비밀번호를 더욱 안전하게 만드는 방법

디지털 여정

사이버 공격을 극복하는 방법

디지털화된 생산 라인을 보호하는 방법

전문가 관점

사이버 보안 보험료를 낮추는 방법

랜섬웨어에 맞서는 데 필요한 것

해커의 관점에서 보안 평가하기

이번 SMB dynamo 편에서 소개한 기술에 대한 자세한 정보가 필요하거나 다음 편에 소개하고 싶은 사례가 있다면 dynamo@cisco.com으로 문의하세요.

중견·중소기업의 사이버 보안을 위한 새로운 동력

대부분의 중견·중소기업은 제약된 인원과 자원으로 비즈니스를 운영하는 것에 집중해야 하기 때문에 사이버 보안과 같은 최신 IT 트렌드를 빠르게 적용하고 위협에 대비하는 것이 어렵습니다. 그렇기 때문에 많은 기업들이 위협이 닥치고 나서야 최소한의 조치를 취하곤 하는 것이 현실입니다.

실제로 점점 더 많은 중견·중소기업이 무방비 상태로 사이버 보안 위협에 노출되고 있으며, IDC는 향후 중견·중소기업의 1/3이 3개월에 한 번씩은 보안 침해를 경험할 것이며, 이것은 평균 일주일 가량 비즈니스를 운영하는 데 지장을 초래할 것이라는 예측까지 내놓고 있습니다.

사이버 범죄자들이 대기업만 해킹하던 시절은 예전 이야기입니다. 오늘날 랜섬웨어 공격은 자동화 되어있을 뿐만 아니라 그 효율성도 극대화 되어 모든 규모의 기업을 공격하고 이익을 취하고 있는 추세입니다. 보안 방식이 상대적으로 취약한 소규모 조직은 오히려 손쉬운 표적이 될 수 있습니다.

이번 SMB dynamo Vol 4.에서는 오늘날 중견·중소기업의 사이버 보안을 유지할 수 있는 새로운 동력이 무엇인지에 대해 살펴봅니다. 점점 더 중요해지는 사이버 보험, "제로 트러스트"의 개념, 그리고 비밀번호의 쇠락에서부터 기업이 랜섬웨어를 막는 방법, 혁신적 도구를 사용하여 잠재적 취약성을 적절한 비용 내에서 찾아내는 방법까지 다양한 주제를 다룹니다. 또한, 스페인의 사례를 통해 가족 경영으로 운영되는 제조업체가 만연한 멀웨어 감염을 극복해낸 과정도 알아볼 것입니다.

대비 하지 않음으로 인해 발생하는 기회 비용은 중견·중소기업에게 그 어느때보다 더 큰 타격을 입힐 수 있습니다. SMB dynamo가 여러분의 비즈니스를 보다 잘 보호하기 위한 방향성을 수립할 수 있도록 도움이 되어 드리겠습니다.

***– SMB dynamo* 편집팀**

기술 동향

맹렬한 공격에 대한 반격

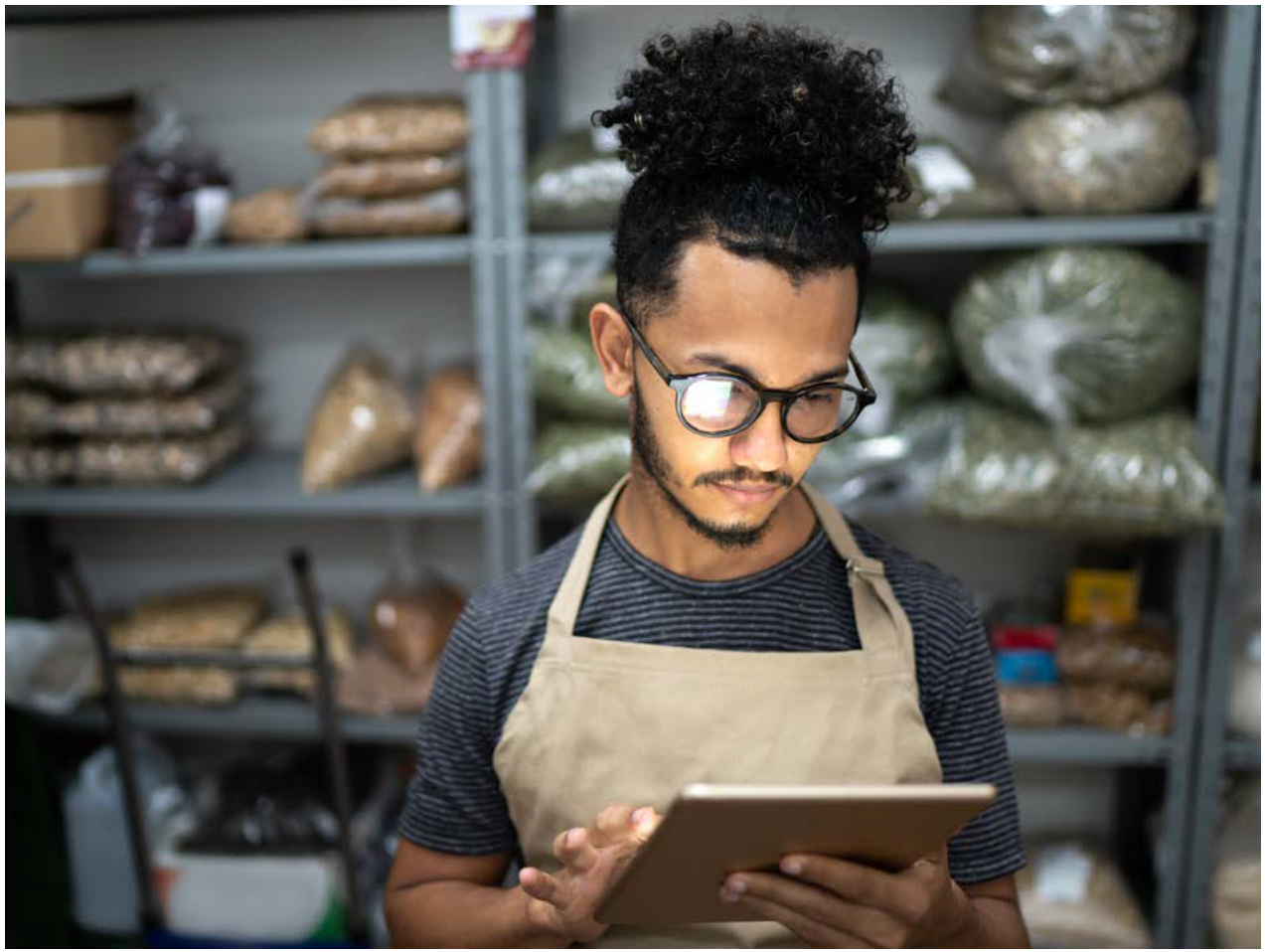
거세지는 사이버 공격에 맞서기 위한 중견·중소기업의 우선 과제

중견·중소기업이 사이버 보안에 철저히 대비하고 있는 경우는 드뭅니다. 2022년 2월, IDC 국제 중견·중소기업 설문조사에 따르면, 해당 규모의 기업 5곳 중 약 2곳만이 정규직 IT 직원(또는 그에 준하는 직원)을 두고 있는 것을 알 수 있습니다. 이들 중견·중소기업에 있는 IT 직원은 대부분 여러 가지 책임을 맡고 여러 방면에서 다양한 업무를 동시에 수행하고 있습니다. 보안은 원래도 복잡한 데다, 보안 자체가 수익 혹은 새로운 고객 유치로 이어지는 것은 아니라는 인식 때문에 기업은 보안 위주의 프로젝트는 잠시 제쳐두는 경우가 많습니다.

하지만 팬데믹을 겪으며 이런 흐름에 변화가 생기고 있습니다. 랜섬웨어와 같은 사이버 공격이 점점 자동화되면서 중견·중소기업들이 오히려 더욱 수익성 좋은 표적이 된 것입니다.

IDC 중견·중소기업 연구 책임자, Katie Evans는 "원격 근무로의 전환은 사이버 공격자들에게 아주 좋은 기회가 되었다"며, 직원이 안전한 보안 장치가 없는 사무실 밖에 나와 멀리 떨어진 위치, 네트워크, 기기에서 비즈니스에 중요한 시스템에 액세스할 때 노출과 위험이 증가한다고 언급했습니다. "중견·중소기업은 IT 보안 기능이 대기업에 비해 덜 성숙한 경우가 많아서 특히 이러한 공격에 취약합니다."

IDC는 최신 조사 결과를 바탕으로 2024년에 중견·중소기업의 33%가 분기에 최소 한번은 IT 보안 침해를 경험하여 일주일 이상 비즈니스 운영에 지장을 겪을 것으로 예측했습니다. 많은 사람이 이 경고에 주의를 기울이기 시작했습니다. Evans는 "조사 대상 중견·중소기업의 절반이 향후 12개월 동안의 기술 우선순위로 보안을 선택했다"고 말했습니다.



그렇다면 어떻게 최소한의 IT 리소스로 보다 강력한 보안을 구축할 수 있을까요?

"다양한 업무를 수행하는 IT 전문가"

중견·중소기업이라고 하면 갓 생겨난 기술 전문 스타트업을 떠올리는 경우가 많습니다. 하지만 사실, 중견·중소기업의 기업가들은 10년도 훨씬 전부터 사업을 구축하기 시작해 종종 IT에 대해 다른 견해를 가지고 있는 경우가 많습니다. IDC의 조사에 따르면, 중견·중소기업의 34%가 10~20년 동안 사업을 운영하였고 36%는 그보다 더 오래 사업을 유지해 온 것으로 드러났습니다. 즉, 이들과 같이 오래된 기업들의 대부분은 크게는 기술, 좁게는 사이버 보안을 주요 비즈니스 우선순위로 생각하지 않을 수 있습니다.

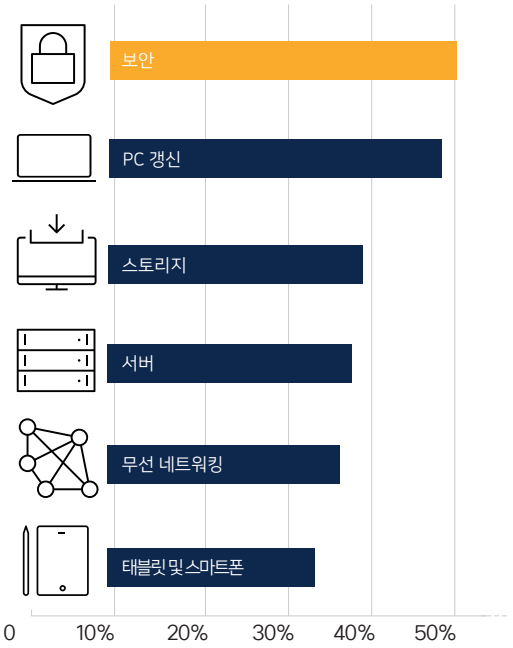
Evans는 "소규모 기업의 IT 전문가는 실로 여러 가지 직무를 겸임합니다. 직원들의 기술적 요구 사항과 문제 해결, 온라인 프레젠스, 서버 및 클라우드 인프라, 금융 및 급여 시스템 , 통신 및 협업 도구, 때로는 POS, 때로는 마케팅 자동화 등에 이르는 모든 것을 책임집니다."라고 이야기합니다.

실제로 IT 보안은 비즈니스 목표를 달성하는 데 가장 큰 장벽으로 여겨지는 경우가 많습니다. IDC가 중견·중소기업들을 대상으로 비즈니스 우선순위를 달성하는 데 가장 큰 기술적 문제가 무엇인지 물었더니 상위 2개의 답변이 보안과 관련이 있었습니다. 보다 구체적으로는, 새로운 기술을 안전하게 구현하는 것과 원격 근무 직원을 안전하게 비즈니스 시스템으로 연결하는 것이었습니다.

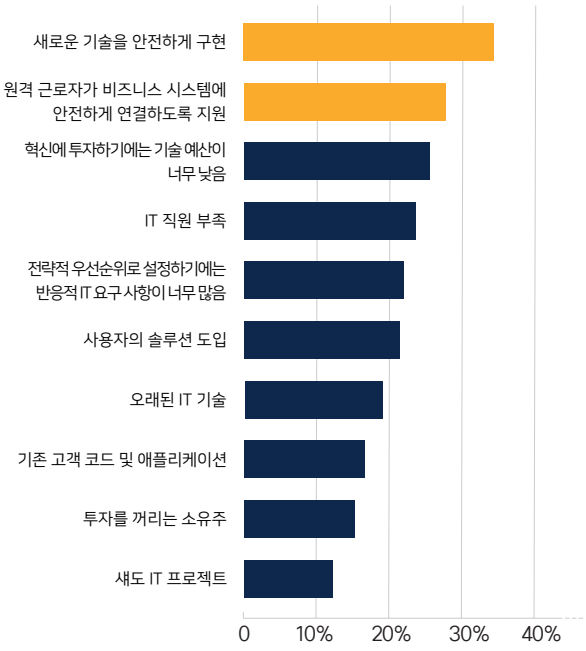
IT 보안은 중견·중소기업의 최우선순위

2024년에 중견·중소기업의 33%는 3개월에 1번씩 보안 침해를 경험하여 일주일 이상 비즈니스 운영에 지장이 발생할 것

다음 중 향후 12개월 동안 귀사의 기술 우선순위가 될 인프라 및 기기는 무엇입니까?



비즈니스 우선순위를 달성하는 데 가장 큰 기술 문제는 무엇입니까?



Source: IDC, 2022 Worldwide Buyer Behavior Snapshot, Doc # US49058522, May 2022

보험으로 인한 보안 요구 사항의 변화

위협에 대비하지 않았을 때의 기회 비용이 상당하기 때문에 이제 중견·중소기업은 사이버 보안을 위한 해답을 찾을 수밖에 없습니다. 치솟는 사이버 보안 보험료 또한 적극적인 대책 마련을 위한 동기부여가 되었습니다. ("사이버 보안 보험으로의 로드맵," 17페이지를 참조하세요.)

Cisco Secure 사이버 전문가, Wolfgang Goerlich는 이런 소식을 자주 듣습니다. 그는 "보험은 요즘 최대의 관심사죠. 예전에는 규제적 혹은 고객의 요구 사항에 따라 보안 체제가 결정되었다면, 이제는 보험사가 보안 방침에 영향을 끼치게 되었습니다. 보험사는 이제 철저한 보안 체제 구축을 장려하고 기본적인 보안 체제의 유지 및 관리를 요구합니다."라고 말했습니다. (Goerlich의 발언에 대한 자세한 내용은 "중견·중소기업이 "제로 트러스트" 보안을 도입하는 방법"(8페이지)을 참조하세요.)

통합된 보안 솔루션

이러한 기술적 동향들은 중견·중소기업들이 지금까지의 IT 보안 조치를 검토하기에 충분한 이유가 됩니다.

"예전에는 규제적 혹은 고객의 요구 사항에 따라 보안 체제가 결정되었다면, 이제는 보험사가 보안 방침에 영향을 끼치게 되었습니다. 보험사는 이제 철저한 보안 체제 구축을 장려하고 기본적인 보안 체제의 유지 및 관리를 요구합니다."

Wolfgang Goerlich
자문 CISO,
Duo 기반 Cisco Secure Access

반가운 소식은 대부분의 중견·중소기업이 이미 항바이러스 소프트웨어, 네트워크 방화벽 또는 클라우드 기반 백업과 복구 등과 같은 일종의 보안 조치를 취하고 있다는 것입니다.

반면 다소 우려되는 사항은, 일반적으로 이러한 보안에 필요한 도구들이 독립적인 솔루션을 모아놓은 것이기 때문에, 제한적인 중견·중소기업의 IT 직원으로는 사이버 보안을 온전히 모니터링하기 어려운 점입니다. 각종 솔루션이 제공하는 수많은 보안 경고를 확인하고 검증하는 데 필요한 시간, 노력, 기술력 등의 한계에 부딪혀 중요할 수 있는 다양한 경고 알림이 간과되는 경우가 다반사입니다.

모든 Cisco Secure 제품군에 포함된, Cisco SecureX는 원래대로라면 따로 떨어져 있을 센서와 탐지 기술을 단일 플랫폼으로 결합시켜 이러한 고민을 해결해줍니다.

"중견·중소기업은 위협을 체감하고 있기 때문에 비즈니스를 보호하고 위협에 대응하기 위한 전략이 필요하다는 것을 알고 있습니다."

Katie Evans
중견·중소기업 연구 책임자, IDC

Cisco Secure 및 타사 보안 솔루션을 하나로 연결하여 통합된 가시성을 확보할 뿐만 아니라 직관적인 자동 제어 방식을 제공합니다.

Cisco Secure X의 총괄 제품 디렉터인 Albert Salazar는 "SecureX는 중견·중소기업의 IT 환경 내에 발생하는 위협을 찾고 우선순위를 결정 및 대응하는 데 필요한 단순성을 제공합니다. 우리 보안 솔루션 중 하나를 사용해 보셨다면 여러 도구의 정보를 한 번에 보는 것이 얼마나 편리한지 알 수 있을 것입니다."

사이버 보안 위협의 복잡성 및 발생 비용이 점점 더 증가하면서 많은 중견·중소기업이 비즈니스를 보호하는 방법을 더욱 열심히 찾고 있습니다.

SecureX에 대해 자세히 알아보기

Cisco Secure 제품과 함께
SecureX를 체험해보려면
대시보드에 있는 배너를 클릭하세요.

IDC의 Evans는 "중견·중소기업은 직접 위협을 눈으로 보고 체감하고 있기 때문에 비즈니스를 보호하기 위한 전략과 위협 발생시 대응을 위한 계획이 필요하다는 것을 인지하고 있습니다"라고 말했습니다. ■

제로 트러스트 보안의 장점을
이해하고 시작하는 방법:

제로 트러스트 워크숍 참석

중견·중소기업이 "제로 트러스트" 보안을 도입하는 방법

Cisco Secure Access by Duo의 최고 정보 보안 책임 자문, J. Wolfgang Goerlich와의 대화

SMB dynamo: "제로 트러스트"는 무엇이고 중견·중소기업에는 왜 중요한가요?

Wolfgang Goerlich: 제로 트러스트는 단순히 IT 업계에서 유행하는 말처럼 들리지만 조직의 기기와 애플리케이션을 보호하기 위한 새로운 전략을 나타냅니다. 제로 트러스트는 회사의 방화벽 너머까지 보호를 확장하는 보안 아키텍처로, 모바일 기기와 클라우드의 연결이 필요한 오늘날 중요합니다. 액세스가 필요한 곳이 어디든 경계를 설정하여 모든 사용자와 기기가 애플리케이션과 데이터에 연결할 때마다 지속적으로 검증됩니다. 무엇보다 중견·중소기업의 경우, 미국 연방 정부 부서와 기관들이 이 전략을 도입하기 시작했다는 사실 자체가 큰 의미를 시사합니다. 이런 종류의 규제는 기관에서 처음 시작되지만, 얼마 지나지 않아 공급망까지 내려와 작은 기업들에도 영향을 미칠 것이기 때문입니다.

SMB dynamo: 중견·중소기업이 제로 트러스트 전략을 도입할 만한 단기적 가치가 있나요?

Goerlich: 어떤 사업주는 "그건 나중에 걱정하겠다"라고 말하기도 합니다. 이런 보안 제어 기능을 준비해두면 나중에 계약을 수주하려고 경쟁할 때 이익이 될 것이라고 말하는 사람도 있었습니다. 사이버 보험료가 증가한 것도 한몫합니다. 대부분 사이버 보험사는 벌써 제로 트러스트의 구성 요소 중 하나인 다단계 인증이 없으면 보장 범위를 갱신하지 않겠다고 말하고 있으며, 제로 트러스트 사례에 관해 묻기 시작했습니다.

즉, 몇 년 내로 보험사에서 제로 트러스트를 요구하는 것은 시간문제입니다.

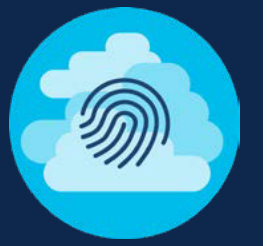
"이런 종류의 규제는 기관에서 시작되지만, 얼마 지나지 않아 공급망까지 내려와 작은 기업에 영향을 미칩니다."

Wolfgang Goerlich
자문 CISO,
Cisco Secure Access by Duo

SMB dynamo: 중견·중소기업을 위한 제로 트러스트 전략은 무엇인가요?

Goerlich: 중견·중소기업에서 제로 트러스트 아키텍처를 만드는 것은 단순한 일이 아니지만 미리 시작할 수 있습니다. 먼저 보안 공급업체와 관리형 서비스 공급업체에 "제로 트러스트 스토리란 무엇이고, 성공하기 위해 가장 명확하고 빠른 경로가 무엇"인지 묻는 것입니다. 크게 보았을 때, 사람, 기기, 네트워크, 애플리케이션 워크로드, 데이터의 5가지 영역이 있습니다. Cisco Secure Access by Duo처럼 어떤 기업이든 쉽고 편리하게 제로 트러스트에 접근할 수 있도록 만든 제품의 경우, 기능만 활성화하면 직원, 기기, 애플리케이션에 적용됩니다. 네트워크와 애플리케이션 워크로드 영역의 경우도 여전히 고려해야 합니다. ■

3가지 요점 정리



1. 사이버 보험사가 제로 트러스트 전략에 관해 묻기 시작
2. 다단계 인증이 제로 트러스트의 구성 요소 중 하나
3. IT가 모든 직원, 기기, 애플리케이션을 잘 보호하고 있는지 질문 시작하기

비밀번호 등의 액세스 문제 해결

중견·중소기업에서 적절한 사용자에게만 적절한 액세스 권한이 부여되었는지 지능적으로 알아보는 방법

비밀번호는 오랫동안 필수로 사용되었지만 결함이 많은 형태의 보안입니다. Verizon의 2022 데이터 보안 침해 조사 보고서에 따르면, 전체 보안 침해의 절반이 자격 증명 도난이나 취약한 자격 증명이 원인이었습니다.

비밀번호로 인한 위험은 팬데믹 중에 더욱 커졌습니다. 시스코의 파트너, Port53 Technologies의 창업자이자 최고 경영자인 Omar Zarabi는 "원격 근무가 대세가 되면서 훨씬 많은 기업이 클라우드로 애플리케이션을 옮겼습니다. 많은 중견·중소기업이 가동 지원을 첫째로, 보안을 두 번째로 놓고 있습니다. 비밀번호의 정글은 더욱 커져서 다루기 어렵게 되었습니다."라고 말했습니다.

비밀번호가 많으면 다른 문제도 악화됩니다. 가장 큰 문제는 사용자가 그 모든 것을 기억하는 데 힘든 시간을 보낸다는 것입니다. Cisco Secure 부서인 Duo Security의 조사에 따르면, 사용자의 51%가 매주 비밀번호를 잊거나 재설정한다고 밝혔고 사용자의 57%가 여러 사이트에 동일한 비밀번호를 재사용한다고 답했습니다.

그와 동시에 사이버 범죄자는 더욱 교묘하게 기업의 비밀번호를 훔치고 있습니다.

피싱을 이용하거나 안전하지 않은 가정 및 공용 Wi-Fi 네트워크를 노리거나 여기에 더해 더욱 자동화된 랜섬웨어 공격을 더해 쉽게 노릴 수 있는 중견·중소기업이 금세 수익을 얻을 수 있는 좋은 표적이 됩니다.

비밀번호는 이러한 싸이클 내에서 매우 위험한 연결 고리가 될 수 있습니다. Zarabi는 "원래대로라면 기업은 네트워크에 공격이 발생할지 걱정해야 했습니다. 지금은 ID와 액세스에 대한 공격을 걱정해야 합니다.

그래서 IT 부서는 항상, 모든 곳을 보호할 방법을 모색해야 합니다."라고 말했습니다.

컨텍스트와 함께 비밀번호 보호하기

생체 인증, 보안 키, 모바일 기기 등을 통해 사용자 ID를 설정하는 것보다는 비밀번호 자체를 모두 교체하는 것이 이상적이지만, 많은 중견·중소기업에서 여전히 효과적인 사이버 보안 전략을 위해 비밀번호가 중요한 역할을 하는 것이 현실입니다.

Zarabi는 "비밀번호에 문제가 많기는 하지만, 중요성이 큽니다. 비밀번호를 보호하려면 다른 액세스 제어 기술을 추가하거나 컨텍스트에 대해 이해하는 것이 중요합니다."

이때 다단계 인증(MFA)이 중요한 기술적 역할을 합니다. MFA는 추가적인 별도의 ID 검증을 시행한 다음, 데이터 및 애플리케이션에 액세스 권한을 부여합니다. 이를 위해 사용자가 아는 것(비밀번호)에 사용자가 가지고 있는 것(휴대전화 알림)을 결합합니다. MFA와 비밀번호를 결합하면 적절한 사람만 적절한 회사 데이터 유형에 액세스할 수 있도록 하는 데 도움이 됩니다.

Cisco Secure Access by Duo의 제품 마케팅 관리자인 Ted Kietzman은 "ID는 새로운 경계입니다. 예전에는 네트워크에 한 번 인증을 통해 액세스 권한을 받을 수 있었습니다. 지금은 기업에서 ID와 기기를 확인하는 것보다는 인증 단계를 세분화해야 합니다."라고 말했습니다.

산업 규정과 보험으로 인해 이런 종류의 보안 방식 사례는 점점 그 필요성이 커지고 있습니다. Kietzman은 "사이버 책임 보험으로 인해 MFA에 대한 대화가 늘어나고 있습니다. 기업에서 보험료를 낮추려면 MFA가 필요합니다."

MFA에 대한 절차

다행히도 많은 중견·중소기업이 이미 특정 애플리케이션이나 플랫폼에 일부 MFA를 사용하고 있으며, 대부분의 직원이 기기를 통한 MFA에 익숙해 지는 추세입니다. 문제는 클라우드든 아니든 IT 환경 내에서 MFA를 일관적으로 사용하는 것입니다.

비밀번호 없는 인증이 모든 규모의 조직에 장점인 이유에 대해 알아보기:

Duo Passwordless: 전문가 팁을 얻고 질문에 대한 답을 얻으세요!

Zarabi는 세 가지로 나눈 핵심 절차를 권합니다.

1단계: 범위 이해 – 먼저 어떤 애플리케이션을 사용 중이고, 어디에 로그인 자격 증명이 필요하고, 어떤 사용자가 사용하는지 감사하는 것으로 시작합니다. 또한, IT에서 애플리케이션을 프로비저닝하는지, 개인적으로 사용하는지 확인합니다. 로그인 활동에 대해 이해하면 MFA가 취약성을 완화하는 방법에 대해 아는 데 도움이 될 수 있습니다.

2단계: 제어 권한 (다시) 확보 – 조직 내에서 Wild West와 같은 비밀번호를 사용하면서 거의 감독을 하지 않을 경우, IT가 자동화된 관리를 통해 제어 권한을 다시 가져올 수 있는 도구를 고려해 보세요.

3단계: 사용하기 편리한 MFA 구현 – 가장 효과적인 보안 도구는 IT와 사용자 모두 매우 사용하기 편리해서 이를 우회할 이유가 그다지 존재하지 않는 도구입니다. 온프레미스, 클라우드, 또는 그 두 가지를 합친 곳에 간단하게 배포되는 MFA 솔루션을 찾아보세요. 현재의 직원과 신입 직원의 등록을 단순화하되, 셀프서비스 옵션을 구현하는 것이 이상적입니다. 모바일 기기로 푸시 알림을 보내는 등, 다양한 2단계 인증 방법을 제공합니다.

결론적으로 비밀번호는 중견·중소기업 보안에서 여전히 하나의 무기로 사용될 가능성이 큽니다. 다행히 이미 새로운 기술을 사용하여 비밀번호 프로그램을 강화하고, 사용자 ID를 더욱 확실히 확인하여 비즈니스 위험을 낮출 수 있습니다. ■

디지털 여정

공기와의 싸움

스페인 제조업체가 사이버 공격을 극복해낸 비결

Enrique Villaverde는 자신의 회사 네트워크가 올바르게 작동하지 않는 것을 알았습니다. 스페인 사라고사에서 그의 가족이 경영하는 로커 제조업체인 Megablok에서 직원들이 데스크톱에서 연결이 끊어지는 경우가 많았습니다. 어떤 직원은 매우 불만이 심해서 연결이 훨씬 안정적인 집에서 일하겠다고 요청하기도 했습니다.

직원 80명을 두고 정규직 IT 직원이 없는 25년 된 기업의 최고 경영자, Vilaverde는 "불만과 불편을 겪으며 여러 달을 보냈습니다. 싸우는 대상이 누구인지, 싸울 방법이 무엇인지도 모르기 때문에 화가 치솟았습니다. 광대역을 확장하고, 케이블 연결을 다시 확인했지만 문제는 지속되었습니다. 마치 공기와 싸우는 것 같았습니다."라고 말했습니다.

팬데믹이 시작되며 스페인이 봉쇄에 들어간 후, 이미 좋지 않았던 상황은 더욱 악화되었습니다. 고객들은 Megablok에서 발행한 듯했으나, 금액을 보낼 은행 계좌 번호가 다른 가짜 청구서를 받기 시작했습니다.

Villaverde는 "이제 우리 생산성이 감소하는 게 문제가 아니었습니다. 우리 이미지가 훼손되고 있었죠. 그때야 경보음이 들렸습니다."라고 말했습니다.

수천 개의 악성 연결

Megablok는 도움을 얻기 위해 사라고사에 있는 시스코 프리미어 파트너인 Orbe Seguridad에게 문의했습니다.

Orbe의 엔지니어링 및 기술 이사인 Daniel Sánchez Yuberto는 발견한 조사 결과에 놀랐습니다. "이 경우, 우리 인시던트 대응팀이 먼저 Cisco Umbrella를 배포하여 모든 DNS 발송 트래픽을 모니터링했습니다. 모든 엔드포인트가 설정한 모든 연결을 관찰하고, 멀웨어, 피싱, 암호화 화폐 채굴, C&C를 제공하는 모든 악성 연결을 차단합니다."

Villaverde나 Sánchez가 상상했던 것보다 상황이 심각했습니다. Sánchez는 "정말 놀라웠습니다. 악성 도메인으로 연결되는 수천 개의 연결이 설정되어 있었습니다."라고 말했습니다.

감염 치료

충격적이기는 하지만 Megablok의 사이버 공격이 그다지 특별한 것은 아닙니다. 팬데믹이 시작되어 2년이 지나는 동안, 많은 기업에서 보안 위험이 금세 커졌습니다. 더욱 많은 직원이 안전하지 않은 네트워크나 개인 기기를 사용해서 재택근무를 시작했기 때문입니다. 또한, 대부분 조직은 재빨리 새로운 기술을 받아들여 운영을 자동화 하거나, 안전 절차를 개선하거나, 원격 액세스를 도입했습니다. 중견·중소기업은 리소스와 IT 전문성이 부족하다는 점을 고려하면 쉬운 표적이 되는 경우가 많습니다.

다행히도 Megablok은 복구 불가능한 피해를 보기 전에 Orbe에게 복구를 요청했습니다. Sánchez의 팀은 매우 신속하게 움직여 엔드포인트를 식별하고 자신도 모르게 악성 트래픽을 보내던 사용자를 찾아냈습니다. Sánchez는 "하루도 안 되어 Megablok 네트워크는 사용 중단 상태에서 벗어날 수 있었습니다.

하지만 Megablok이 매일 수백 통씩 받는 피싱 이메일을 포함한 여러 가지 보안 문제들이 여전히 남아 있었습니다. 직원들은 어떤 이메일이 정상인지 알 수 없었고, 이는 고객 관계에 부정적 영향을 미치기 시작했습니다.

가짜 청구서는 어떻게 된 일이냐구요? 이는 사이버 범죄자가 일부 기업 직원의 자격 증명을 훔치는 이른바 "중간자 공격"의 피해를 보았을 가능성이 큽니다. 피해자의 이메일을 읽고 피해자의 도메인 이름과 매우 유사하게 사용하는 이메일을 사용하여 대응하고, 별칭으로 표시한 후, 마치 Megablok을 대표하는 것처럼 효과적으로 소통할 수 있습니다.

Orbe는 Megablok의 받은 편지함을 보호하기 위해 클라우드 기반 Cisco Secure Email을 배포하고 모든 사용자에게 자격 증명을 업데이트할 것을 지시했습니다. 거의 하룻밤사이에 피싱 이메일의 양이 급격히 하락했습니다. 이제 사용자는 갑자기 다시 이메일을 신뢰할 수 있게 되고 비즈니스 운영에 집중 할 수 있게 되었습니다.

마지막으로, Orbe는 여러 엔드포인트를 감염시킨 멀웨어를 제거해야 했습니다. Sánchez는 Cisco Secure EndPoint를 구성하고 배포했습니다.

Cisco SecureX에 모든 솔루션을 통합하여, 쉽게 위협을 조사하고 감염된 엔드포인트를 분리하고, 설치된 멀웨어를 제거해야 했습니다."라고 말했습니다.

회복 자금 지원

Megablok의 운영을 개선한 효과는 즉각적이었습니다. 연결 문제가 사라졌고, Villaverde는 인프라를 더욱 잘 보호하고 안심할 수 있었습니다.

리소스가 부족한 여느 소규모 기업과 마찬가지로, 이런 보호 조치를 위한 투자에는 신중한 고려가 필요했습니다. Villaverde는 "공격에서 회복하고 회사의 생산성을 유지하려면 새로운 기술을 도입해야 한다는 것을 알았습니다. 하지만 규모가 작은 가족 경영 사업이다보니 비용을 책정하는 것이 부담스러웠습니다."라고 말했습니다.

Orbe는 Villaverde를 Cisco Capital로 연결해주었고, 이 센터에서 글로벌 공급업체 자금 지원 기관인 DLL과 협력하여 Megablock에 가장 적절하고 유연한 지불 방법을 찾았습니다. 따라서 Villaverde의 회사는 프로젝트의 총소유비용을 간소화하고 Orbe의 관리형 서비스를 예측 가능한 지불 방법으로 합치고 미리 선불 비용을 낼 필요가 없게 되었습니다.

Villaverde는 "장기적으로 일정 금액을 지불하면 다른 비즈니스 자산을 줄일 필요가 없고, 예산을 더욱 잘 관리할 수 있습니다."라고 말했습니다.

Megablok이 보안 침해에서 벗어나서 Villaverde를 비롯한 직원들은 다시 한번 걱정 없이 일할 수 있게 되었습니다. Villaverde는 "이제 우리가 정말로 해야 할 일을 돌보러 갈 수 있게 되었습니다. 우리 부모님과 여동생, 제가 25년 전에 만든 가족의 레거시 말이죠."라고 말했습니다.■

Orbe Seguridad가 어떻게 관리형 사이버 보안 서비스로 중견·중소기업을 보호하는지 자세히 알아보세요.

전체 영상 보기:

Orbe Seguridad의 4단계 회복 계획

1. 네트워크 중단 해결
- **Cisco Umbrella**로 모든 DNS 발송 트래픽을 모니터링하여 모든 엔드포인트에서 설정한 전체 네트워크 관찰

2. 이메일을 중요한 채널로 보호
- **Cisco Secure Email** 배포 및 모든 액세스 자격 증명 업데이트

3. 엔드포인트에서 멀웨어 제거
- **Cisco Secure EndPoint** 구성 및 배포

4. 하나의 플랫폼에서 통합
- **Cisco SecureX**를 하나의 보안 관리 시스템으로 삼아 더욱 손쉽게 지속적으로 모니터링 실시

Cisco IoT 및 Vem Sistemi가 중견·중소기업을 관리하고 사이버 위험을 완화하도록 돕는 방법을 자세히 알아보세요.

스마트 공장을 위한 안전한 네트워크

제조사 DECO Industrie가 디지털화된 생산 라인을 보호하는 방법

휴대전화, 노트북, 프린터를 업그레이드하는 것과 별개로 수십 년간 사용하던 산업 장비를 현대화하는 문제는 다릅니다.

DECO Industrie는 1951년에 첫 공장을 열었습니다. 이 이탈리아 제조업체는 그 이후로 느리지만 꾸준히 성장하며 가정용 세척제에서 식품, 미용 제품으로 영역을 확장했습니다. 현재 이 기업은 6개의 생산 공장을 두고 있으며, 모든 공장이 대규모 공장 설정에 맞춘 기술로 현대화를 꾀하고 있으나 중견·중소기업 제조업체에서 감당할 만한 수준의 요금과 단순성을 적용하고 있습니다.

DECO Industrie 대표, Antonio Campri는 "우리는 언제나 새로운 시장에서 성장하고, 품질을 모니터링하고, 비용을 관리하고, 생산성을 개선할 새로운 기술에 관심이 많습니다."라고 말했습니다.

실시간 산업 데이터

최근 들어 이 회사는 생산 라인의 장비를 업그레이드하여 인터넷 및 상호 연결을 할 수 있도록 하고, 강화된 산업 환경용으로 설계된 Cisco IoT network와 연결했습니다. DECO Industries는 71년 역사상 처음으로 공장을 한눈에 보고, 비즈니스 운영에 영향을 미치고 최적화하는 데 도움이 되는 실시간 데이터를 제공받을 수 있게 되었습니다.

DECO Industries의 IT 서비스 공급업체이자 Cisco Gold 인증 파트너인 Vem Sistemi의 혁신 책임자, Marco Bubani는 "DECO는 생산 공장에서 더 많은 데이터를 얻을수록, 효율성과 품질이 높아진다는 것을 압니다."라고 말했습니다.

연결성의 보호

하지만 연결에 취약성이 있어서 회사에서는 산업 네트워크와 장비를 여러 보안 솔루션으로 강화해야 했습니다.

Cisco Identity Services Engine(ISE)은 네트워크에 누가, 언제 액세스하는지 모니터링하고 제어하는 데 도움이 됩니다.

Cisco Industrial Network Director(IND)는 공장 자동화 기기와 프로세스를 한눈에 볼 수 있습니다. Cisco Industrial Security Appliances(ISA)는 모든 장비를 악성 또는 원치 않는 작업으로부터 보호합니다.

Bubani는 "범용 네트워크 인프라는 DECO의 디지털 여정을 지원할 수 없습니다. 산업 환경, 기기, 애플리케이션용으로 설계된 공장 중심적 네트워크 인프라가 필요했습니다."라고 설명했습니다.

IoT 네트워크는 DECO Industrie의 회사 네트워크로부터 완전히 분리되어 회사 공장 환경과 비즈니스 사무실 사이에 데이터를 안전하게 교환할 수 있는 "산업용 DMZ"를 두었습니다.

Campri는 "기술을 통해 장비와 인간이 대화할 기회를 놓칠 수 없었습니다."라고 말했습니다. 더욱 지능적인 제조를 위해 최신 기술을 안전하게 배포할 방법을 찾는다면 이 70년 된 기업이 다시 70년 동안 성장하는 데 도움이 될 전략을 찾는 것이기도 합니다. ■

전문가 관점

사이버 보안 보험으로 향하는 로드맵

보안을 최대화하고 보험료를 최소화하는 방법

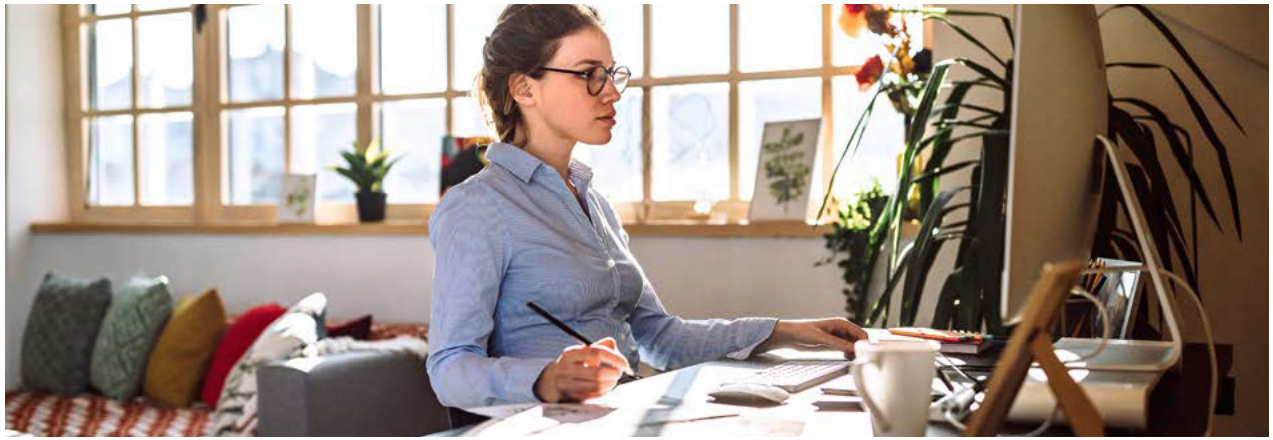
Ed Zarrell이 최근 들어 기업의 경영자들과 대화를 나누는 동안 같은 주제가 계속 화제에 올랐습니다. 바로, 사이버 보안 보험입니다. 로스앤젤레스의 시스코 파트너 LA Networks의 영업 이사, Zarrell이 "오늘날 대부분의 기업 운영자들은 랜섬웨어나 데이터 침해를 입은 주변 기업을 알고 있거나 적어도 들어본 경험이 있을 것입니다. 다양한 사례들에 대한 우려와 사라지지 않을 랜섬웨어에 대한 대응책으로 사이버 보안 보험에 대한 관심이 커지고 있습니다."라고 말했습니다.

이런 우려는 당연합니다. 사이버 보함 제공업체

Coalition에 따르면, 중견·중소기업이 원격 근무로 전환하고 나서 2020년 랜섬웨어 쓰나미가 온 후에, 2021년에는 소규모 기업에 대한 랜섬웨어 공격이 그 전 해보다 40% 늘었습니다. 이에 2021년에 사이버 보험의 평균 보험료는 56% 상승했습니다.

대규모 조직이 한때는 사이버 범죄의 주요 타겟이었으나, 최근 공격 사례들은 더더욱 자동화되었으며 보안에 취약한 중소기업이 수익성 좋은 표적이 되었습니다. Zarrell이 말했듯, "사이버 공격으로부터 자유로운 조직은 어디에도 없습니다."

사이버 공격이 발생했을 때 적절한 보험 정책이 있으면 잠재적으로 엄청난 비용을 초래하는 재무적 지출을 완화하고 비즈니스 중단, 법무 비용, 포렌식 분석 등의 비용을 커버하여 안심할 수 있습니다. 그러나 보험에 가입하는 것도 나름의 단점이 있습니다.

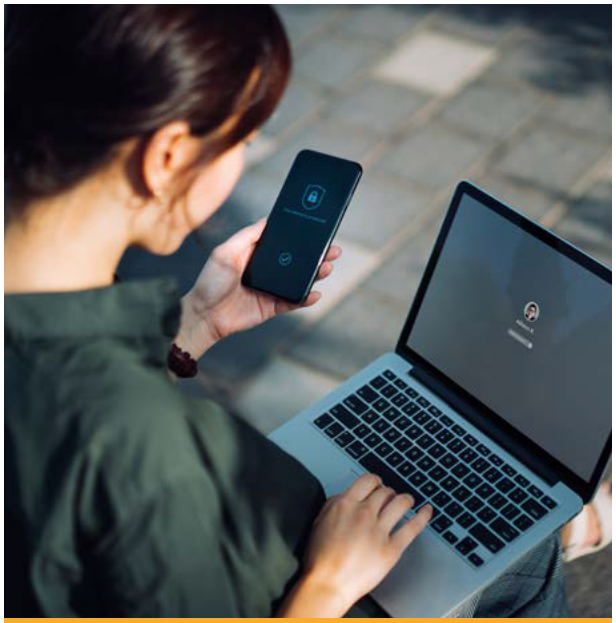


값비싼 보험료, 하지만 공격을 받으면 더 큰 대가를 치러

사이버 보안 보험을 원하는 중견·중소기업은 비싼 요금에 충격을 받는 경우가 많습니다. 보험사에서 폭증하는 청구 속에서 위험을 예측하는 데 어려움을 겪자 보험료가 치솟았기 때문입니다.

보한 브로커 Brown & Brown의 사이버 보험 부사장인 Cole Haney에 따르면, 보험료는 최근 들어 랜섬웨어의 증가로 두 배 이상 올랐습니다. 보험료가 올랐음에도 불구하고 여전히 많은 중견·중소기업이 보험을 통해 비즈니스가 해킹당하지 않을 것이란 마음의 평화를 얻습니다. 하지만 기업이 보험에 가입할 자격을 갖추더라도 보험사는 공격이 발생하지 않도록 막기 위한 더욱 엄격한 IT 보안 기준을 이행할 것을 요구합니다.

Haney는 "사이버 보험 가입 자격을 채우는 데 어려움을 겪고 있거나, 평균 이상의 보험료를 내거나, 보장 범위에서 제외되는 여러 가지 항목을 보게 된다면, 보안 태세를 평가하고 보안을 강화할 수 있는 도구와 제어 기능을 고려해야 한다는 강력한 신호입니다."라고 말했습니다.



사이버 보험사에서 요구하는 5가지 필수 보안 대책

1. 다단계 인증
2. 엔드포인트 탐지 및 대응
3. 데이터 백업 및 복구 전략
4. 원격 액세스 보호
5. 차세대 방화벽

MFA로 시작하기

Haney는 보험료를 낮추는 가장 단순하면서도 효과적인 도구이자, 보험 가입 자격이 아니더라도 점점 필수적인 요구 사항으로 자리 잡은 도구로 다단계 인증(MFA)을 꼽습니다. 미국 국가 보안 사이버 책임자 Anne Neuberger에 따르면, 애플리케이션 및 IT 시스템 액세스 시 두 가지 이상의 ID 인증을 의무화합니다. 주로 휴대전화나 토큰을 Cisco Secure Access by Duo와 같은 도구와 함께 사용하면 사이버 공격의 90%까지 예방할 수 있습니다. Haney는 "보험사는 MFA가 조직의 보험 가입 자격을 선별하는 데 무엇보다도 중요한 요소입니다. MFA가 없다면 기본적으로 네트워크의 문을 잠그지 않고 두는 것과 같습니다."라고 말했습니다.

하지만 MFA는 보험사에서 요구하는 사이버 보안의 초석 중 하나일 뿐입니다. Haney는 비즈니스에 필요한 3가지 요소를 언급했습니다. 엔드포인트 탐지와 대응은 모든 IT 환경에서 위협을 식별합니다. 데이터 백업과 복구 계획은 일정한 간격으로 백업합니다. 원격 데스크톱 프로토콜은 회사 방화벽 밖에 노출되지 않아야 합니다.

보험사는 위험을 평가하고 보장 범위에 요금을 매기기 위해, 중견·중소기업이 철저한 평가를 거치도록 합니다. Haney는 중견·중소기업이 보안 격차를 찾는 데도 도움이 될 수 있다고 말합니다. "직원 교육 수준을 평가 중입니다. 예를 들어, 직원의 피싱 기술에 대한 인식을 알아보거나, 소프트웨어 패치 절차, 권한 있는 계정 관리 및 이메일 필터링 등의 기능을 제공하는 도구가 있는지 확인합니다."

LA Networks의 사이버 보안 보험 접근법 읽어보기

웨비나 시청,

웨비나 시청, 사이버 보험과 MFA: 여러분이 알아두어야 할 것

충분한 값어치를 하는 보안

적절한 파트너와 협력하면 거쳐야 할 단계를 단순화하는 데 도움이 될 수 있습니다. LA Networks는 스스로 사이버 보안 평가 도구를 개발하여 고객의 보안 프로필에 대한 종합적인 정보를 수집하고, 취약점을 식별하고, 장단기에 걸쳐 취약점을 해결하기 위한 로드맵을 작성합니다. Zarrell은 "적절한 전략만 있다면 아무리 작은 기업이라도 매우 안전한 다계층 보안을 준비할 수 있습니다."라고 말했습니다. (웹사이트에서 미니 평가 샘플 제공.)

기업 리더는 사이버 보안 요구 사항을 부담스럽게 느낄 수 있지만, Zarrell은 적절한 도구를 갖춘다면 그 값어치를 한다고 생각합니다. 큰 비용이 들어가는 사이버 공격이 발생할 가능성을 극적으로 낮출 수 있을 뿐만 아니라, 기업이 훨씬 저렴한 보험료를 지불하는 데도 도움이 됩니다.

Zarrell은 "예를 들어 Cisco Secure 솔루션(예: Duo for MFA, Cisco Umbrella for DNS 웹 보안, 차세대 방화벽, 효과적인 안티바이러스 보호)을 갖추고 있다면 이렇게 구현이 간편한 도구를 사용하여 사이버 보안에 가입하기에 훨씬 유리한 조건을 갖추고 비교적 낮은 보험료를 지불할 수 있습니다."라고 말했습니다. ■

랜섬웨어와의 전쟁

1차 및 마지막 방어선이 모두 필요한 이유

조직을 보호할 간단한 방법 알아보기:

Cisco Umbrella

소규모 기업 엔드포인트 보안

Cisco SecureX

글: 시스코 보안 기술 책임자. Eric Howard

랜섬웨어 공격은 그 어느 때보다 빠른 속도로 다가옵니다. Cisco Secure의 조사에 따르면, 공격자는 점점 자동화되는 프로세스를 사용하여 시스템을 감염시켜, 데이터를 암호화하고, 랜섬 서신을 전송하는 작업을 몇 시간, 이르면 몇 분 이내에 끝낼 수 있습니다.

소규모 기업은 이렇게 빠르게 움직이는 것으로부터 어떻게 보호할 수 있을까요? 먼저, 이들 공격의 원리를 알면 도움이 됩니다.

공격의 원리

랜섬웨어는 IT 시스템으로 다단계 침입이 이루어진 결과입니다. 공격자가 시스템에 대한 액세스 권한을 얻고 랜섬을 지불할 때까지 시스템을 잠그는 행위에는 여러 가지 구성 요소가 포함됩니다.

사용자가 악성 웹 링크(주로 이메일에 있음)를 클릭하면 시작되어, Word 문서나 PDF처럼 보이지만 사실은 1) 정보를 훔치고 2) 공격자에게 기기에 대한 제어 권한을 넘기는 무기화된 파일을 전송합니다.

하지만 랜섬웨어는 하나의 기기에 대한 랜섬을 받는 데 만족하지 않습니다. 따라서 랜섬웨어 공격은 이 기기를 활용하여 다른 기기에서도 추가적인 익스플로잇을 실행하고 네트워크 깊이까지 침투하여, Active Directory 도메인 컨트롤러나 메인 서버에 대한 액세스 권한을 얻습니다.

방어 조정

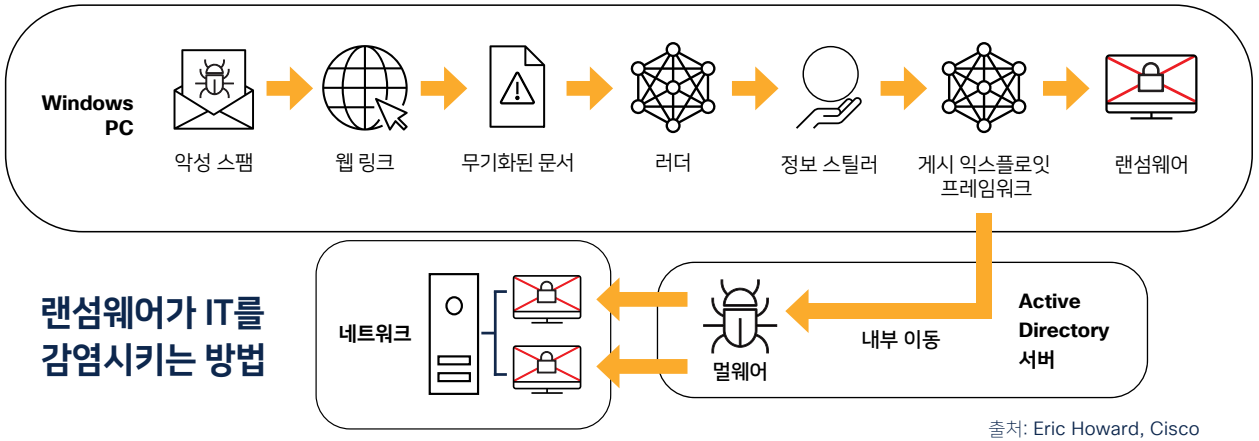
1차 방어선은 웹 트래픽을 모니터링하여 악성 링크로 연결된 것을 차단하는 것입니다. DNS(도메인 이름 시스템)는 도메인 이름을 IP 주소에 매핑하는 인터넷 프로토콜입니다. DNS 검사는 모든 연결 시도의 첫 단계입니다. 기기를 IP와 연결하여 데이터를 받기 전에, DNS 검색이 발생합니다.

DNS 익스플로잇은 감염 또는 제어를 목적으로 랜섬웨어 공격에 섞습니다. DNS 모니터링을 사용하여 Cisco Umbrella와 같은 보안 솔루션을 통해 모든 DNS 검사를 포워딩하면 네트워크의 기기로 다시 연결하기 전에 위협을 차단할 수 있습니다.

마지막 방어선은 엔드포인트 보안으로, 네트워크에 연결된 기기에서 실행되는 잠재적 악성 프로세스를 모니터링합니다.

자동화된 워크플로를 제공하는 Cisco Secure X를 사용하여 DNS 모니터링과 엔드포인트 보안을 함께 활용함으로써, 보안 전문가나 파트너가 의심스러운 웹 트래픽과 DNS 검사를 시작시킨 기기 사이의 관계를 효율적으로 연결할 수 있습니다.

이 두 가지 중요한 보안 도구는 빠르게 움직이는 랜섬웨어에 대해서 랜섬웨어가 확산되기 전에 감염을 격리하는 데 필요한 정보를 제공합니다. ■



출처: Eric Howard, Cisco

해커의 사고로 보안 평가하기

새로운 온라인 도구가 적정 가격의 침투 테스트를 제공할 수 있는 이유

Port53 침투 테스트 서비스가 선제적 보안 태세를 갖추는 데 도움이 되는 이유를 알아보세요.

"알기 전까지는 자신이 무엇을 모르는지 모른다."

이 격언이 사이버 보안에도 적용되는 것은 확실합니다. 어떤 회사의 취약성과 위험은 찾아내서 완화하기 전까지는 지속되고 악용될 가능성이 큽니다.

하지만 회사의 시스템과 데이터가 어떻게 노출되었는지 알 수 있을까요? 한 가지 검증된 전략은 시뮬레이션된 사이버 공격을 승인하고 어떤 일이 일어나는지 살펴보는 것입니다.

이 방법은 많은 대기업에서 사용합니다. 기술 전문가와 충분한 재무 리소스를 갖춘 대기업들은 지속적으로 정기적 침투 테스트를 평가하고 보안을 강화합니다. 하지만 중소기업은 이런 고급 "침투 테스트"는 꿈꾸지 못하는 경우가 대부분입니다.

샌프란시스코에서 소규모 기업이 엔터프라이즈급 클라우드 보안 솔루션을 활용하도록 돕는 시스코 파트너, Port53 Technologies의 창립자이자 최고 경영자인 Omar Zarabi는 "중견·중소기업은 더욱 깊이 있고 빈도를 늘린 평가를 수행하여 보안 틈새를 찾아내야 한다는 것을 압니다. 그러나 기존 침투 테스트는 매우 수동적이고, 최대 6주까지 걸리는 데다 감당하지 못할 정도로 비쌉니다."라고 말했습니다.

따라서 대부분 중견·중소기업은 보안 평가 자체를 피합니다. 규정 준수, 보험, 법적 요구 사항 때문이든 사이버 보안 보호 상태를 검증하는 데 필요한 평가는 일반적으로 빠르고, 비정기적인 취약성 스캔을 통해 한정된 정보만 제공합니다.

Zarabi는 "취약성 검사는 집에 있는 모든 문과 창문이 잠겨 있는지 확인하는 것과 같습니다. 침투 테스트는 그보다 깊이 들어가 누군가 들어왔을 때 무엇을 해킹할 수 있는지 파악해야 합니다. 두 가지 모두 매우 중요하므로 중견·중소기업이 접근하기 쉽게 만들어야 합니다."라고 말했습니다.

이는 그냥 하는 말이 아닙니다.

Port53는 조만간 클라우드 기반의 매우 자동화된 도구를 출시하여 외부 취약성 스캔과 내부 침투 테스트를 수행하고자 합니다. Zarabi에 따르면, 이 도구는 Cisco SecureX와 통합하여 새로 찾아낸 보안 틈새에 대해 수정 사항과 패치 배포를 자동화한다고 합니다.

Zarabi는 "이런 테스트를 자동화하고 클라우드에서 제공하는 것은 상당히 혁명적입니다."라며, 이 도구가 안전한 연결을 통해 IP 주소와 침투 테스트를 사용하여 취약성 스캔을 수행한다고

언급했습니다. "인간과 번거로운 수작업 프로세스를 빼면 중견·중소기업에서 더욱 수시로, 깊이 있는 테스트가 가능합니다. 일부만 알려주는 특정 시점의 정보보다는 언제나 지속적이고 종합적으로 취약성을 이해하는 편이 낫습니다."

무엇보다도, 알기 전까지는 자신이 무엇을 모르는지 모르는 법이니까요. ■