5단계 랜섬웨어 방어

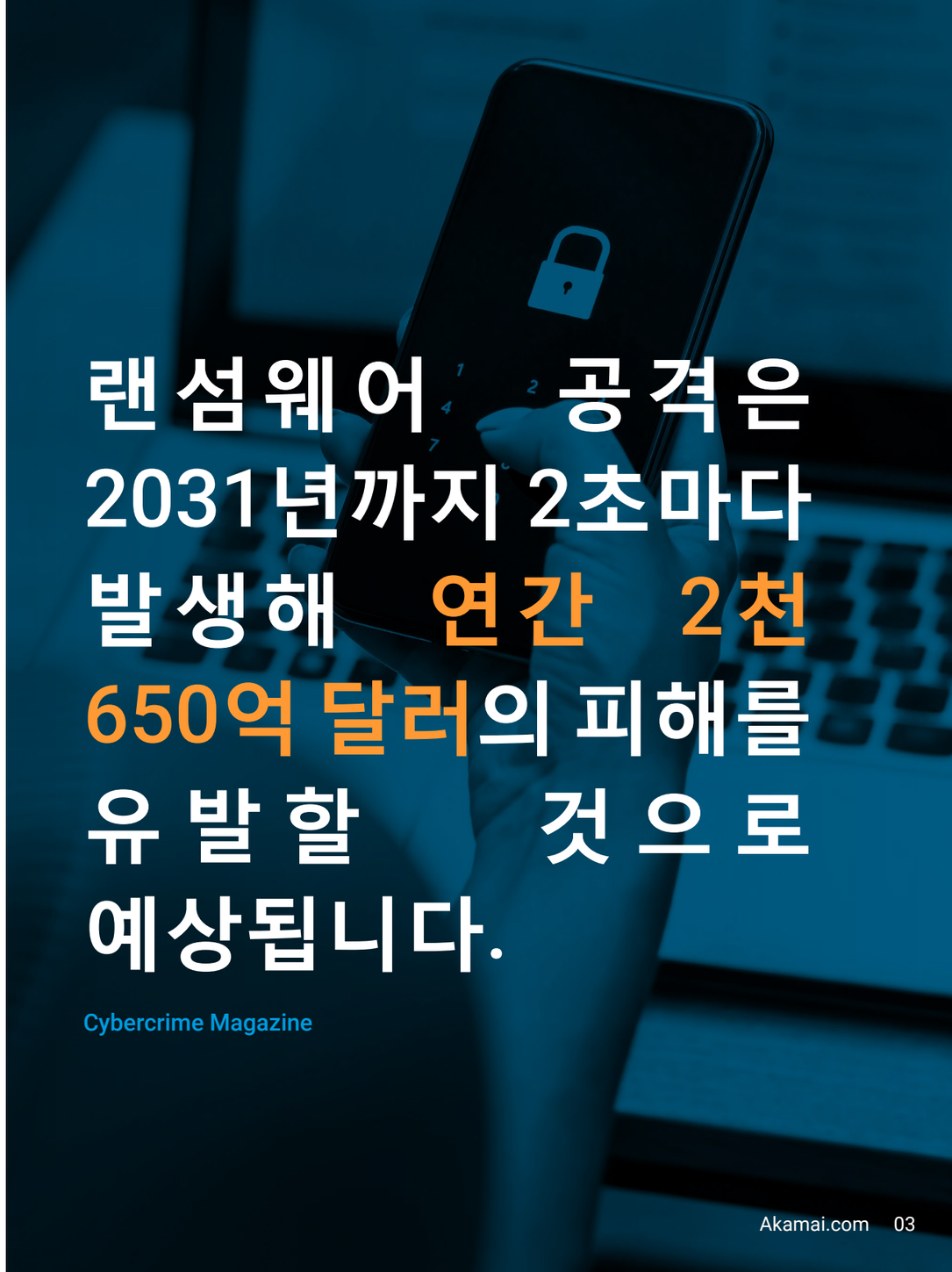
경계를 넘어 방어를 강화하는 방법

목차

서론

랜섬웨어의 증가와 확산

한때 공격자들이 암호화를 통해 파일 및 데이터 접속을 제한하기 위해 사용한 멀웨어의 성가신 변종에 불과했던 랜섬웨어는 막대한 규모의 공격 방법으로 진화했습니다. 영구적인 데이터 손실의 위협도 충격적이지만, 사이버 범죄자와 국가의 지원을 받는 해커들은 랜섬웨어를 이용해 대기업, 주 정부와 지방 정부, 글로벌 인프라, 헬스케어 기업 등에 침투해 마비시킬 정도로 정교해졌습니다. 이러한 기관 중 다수는 RaaS(Ransomware as a Service) 서비스도 외주로 제공하고 있었습니다.



랜섬웨어 공격은 2031년까지 2초마다 발생해 연간 2천 650억 달러의 피해를 유발할 것으로 예상됩니다.

Cybercrime Magazine

재산 피해를 야기하는 랜섬웨어 비즈니스

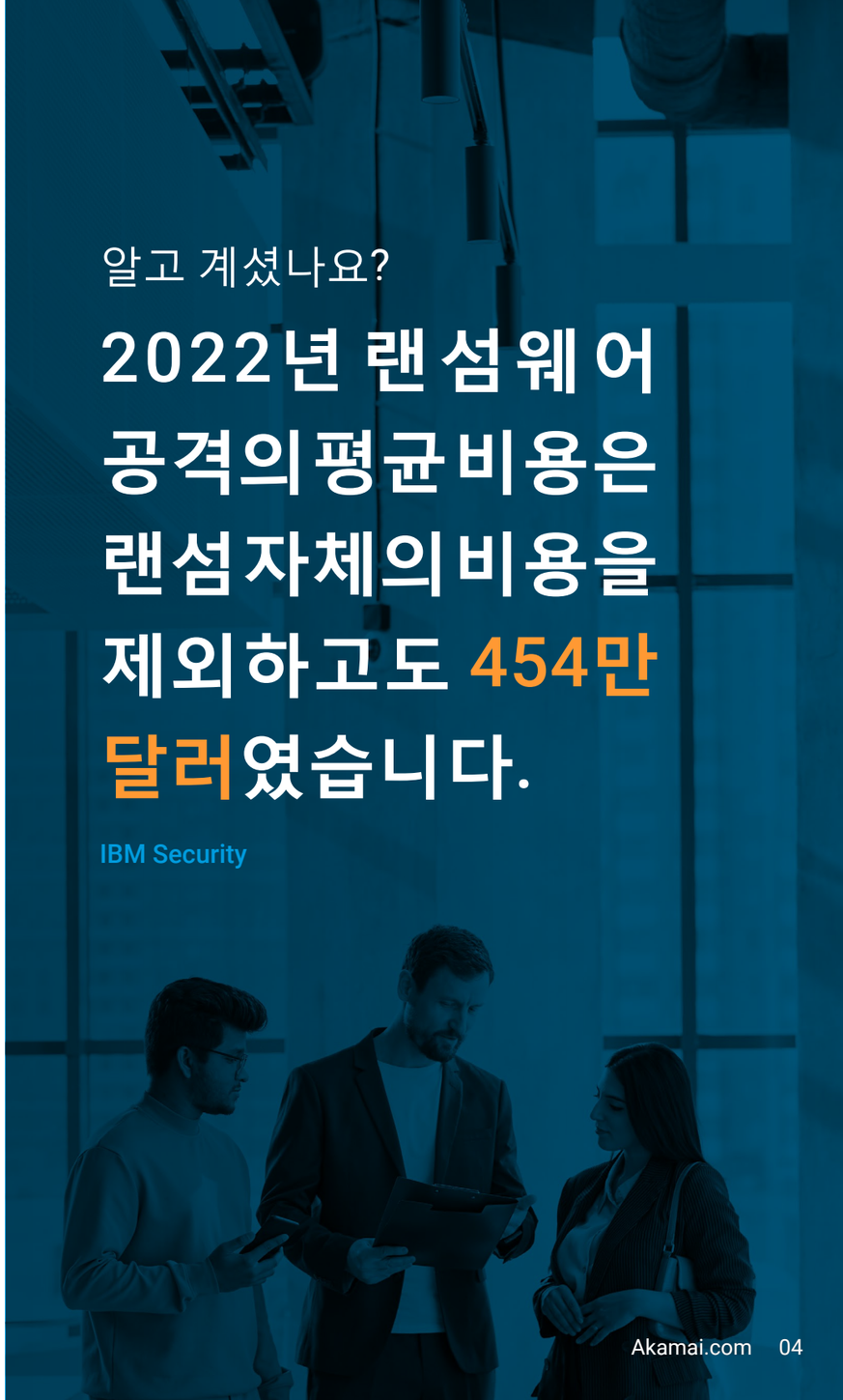
7-Eleven은 2022년 랜섬웨어 공격으로 인해 175개의 매장 운영을 중단했습니다. 현금 등록기를 사용하거나 결제를 승인할 수 없었기 때문입니다. 그 해 초, 독일의 한 석유 회사에 대한 BlackCat 랜섬웨어 공격이 233개 주유소에 영향을 미쳤고, 이로 인해 Royal Dutch Shell은 배송 경로를 다른 저유소로 변경해야 했습니다. 2021년 5월에는 Colonial Pipeline에 공격이 감행되어 미국 동부 연안 전역에서 석유 및 가스 공급이 중단되었습니다. 그리고 2020년에는 Snake 랜섬웨어 공격으로 Honda의 글로벌 운영이 중단되었습니다.

현재 오래된 기술, 경계와 엔드포인트에만 초점을 맞추는 '충분한(good enough)' 방어 전략, 교육과 보안 에티켓의 부재, 알려진 '만능(silver bullet)' 해결책의 부재 등 여러 요인으로 인해 규모를 막론하고 모든 기업이 위험에 처해 있습니다. 사이버 범죄자들은 수천에서 수백만 달러에 이르는 랜섬을 요구하기 위해 최대한 많은 기업 네트워크를 암호화하고 이를 돈벌이 수단으로 삼고 있습니다.

그러나 이로 인해 수익만 위태로워지는 것이 아닙니다. 랜섬웨어 공격의 여파로 인한 다운타임은 비즈니스 운영을 중단시키고 생산성을 저해하며 데이터를 감염시킬 수 있습니다.

기업 비밀 데이터가 유출되거나 감염되면 브랜드가 타격을 입고 고객 충성도가 하락할 수 있습니다. 2020년의 설문조사에 따르면 데이터 유출 사고 중 80%에서 고객 개인 식별 정보(PII)가 유출되었고, 유출 사고의 32%에서 지적 재산이 감염되었으며, 유출 사고의 24%에서 익명화된 고객 데이터가 감염되었습니다. 게다가 공격자들은 이러한 민감한 데이터를 이용해 비즈니스에 피해를 주거나 기밀 데이터 판매를 비롯한 다른 교묘한 행위를 할 수도 있습니다.

랜섬웨어는 네트워크를 통해 빠르게 전파되는 위협입니다. 따라서 이에 맞서 경계만 보호하는 것만으로는 충분하지 않습니다.



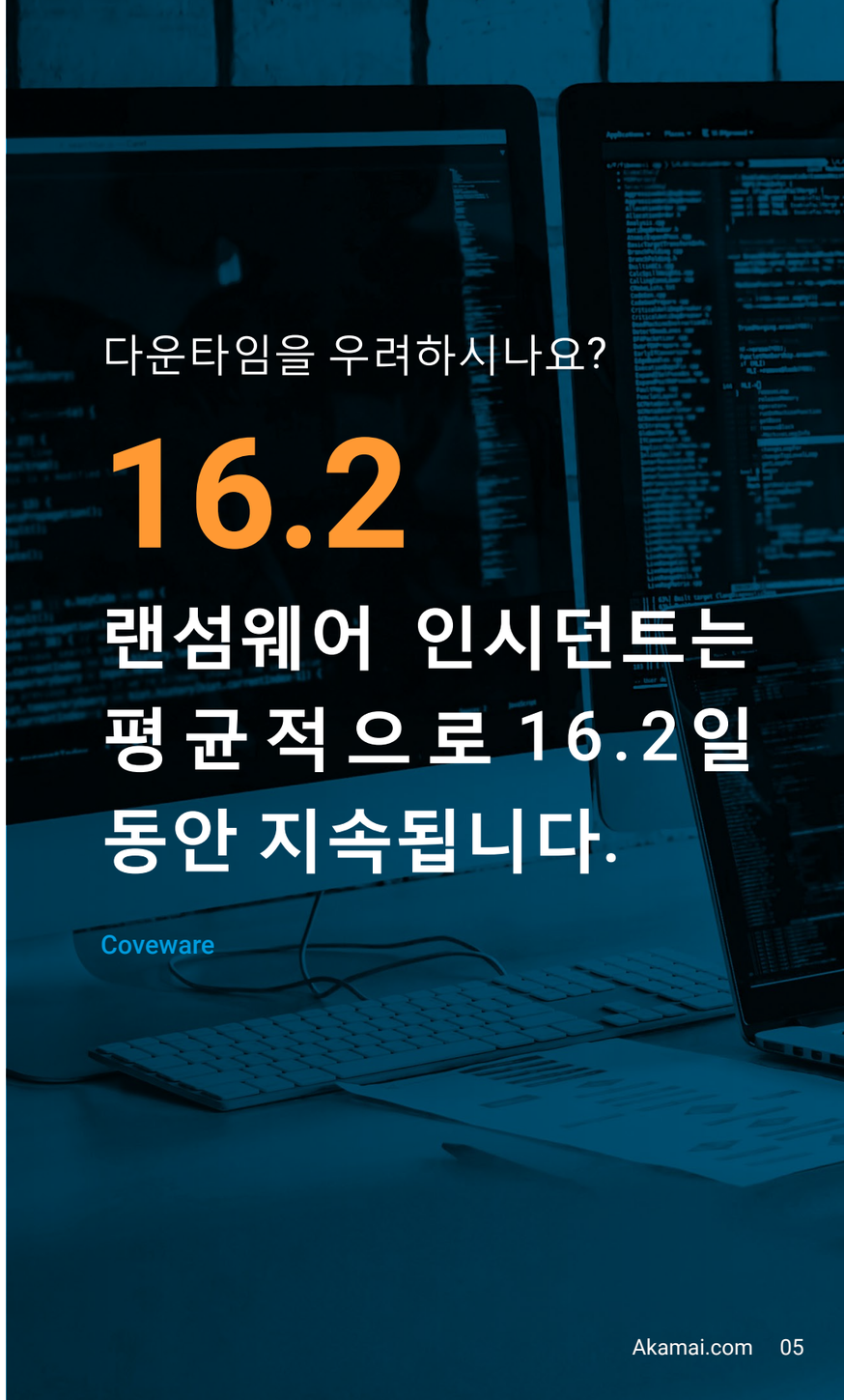
측면 이동과 랜섬웨어 확산을 차단하세요

랜섬웨어 공격은 피싱 이메일, 네트워크 경계의 취약점, 무차별 대입 공격 등 최초의 유출로부터 시작되며 공격자의 실제 의도와 무관하게 보안 체계를 무너뜨립니다.

일단 공격이 디바이스나 애플리케이션에 도착하면 네트워크와 여러 엔드포인트에서 측면 이동을 진행해 감염과 암호화 포인트를 극대화합니다. 공격자는 일반적으로 도메인 컨트롤러를 장악하고 인증정보를 감염시킨 후에 백업을 찾아 암호화해 운영자가 중단된 서비스를 복원하지 못하도록 합니다.

측면 이동은 공격 성공에 매우 중요합니다. 멀웨어가 도착 지점을 넘어 확산되지 않으면 무용지물입니다. 따라서 반드시 측면 이동을 차단해야 합니다.

얼마나 포괄적인 랜섬웨어 위협 방어 전략을 세우고 계십니까?



리스크 방어

철통 같은 방어 전략 구축

네트워크 내부의 측면 이동 탐지 및 방지는 두 가지 주요 중점 분야로 요약됩니다. 먼저 **초기 공격 기법을 약화**시킨 다음, **전파 경로를 제한**하는 것입니다.

인터넷에 노출되는 서버의 양을 제한하고, 공격표면 축소를 위해 지속적으로 패치를 관리하며, 링펜싱을 통해 애플리케이션 간의 전파 경로를 줄이고, 공격이 발생할 경우 신속하게 온라인으로 복귀하고 광범위한 데이터 손실을 방지할 수 있도록 데이터를 백업하는 것 등의 조치를 취할 수 있습니다.

보안 계획에 우선순위를 부여하는 네 가지 방법

기업의 광범위한 대응 전략, 계획 수립, 예산에 보안을 포함해야 합니다. 즉, 최고 경영진 수준 임원 및 이사진의 인식을 제고하고, 잠재적 리스크와 이를 방어하기 위해 필요한 사항에 대한 경계를 늦추지 않아야 하는 것입니다.

1. 기업의 전반적인 리스크 방어를 관리하는 기능에 사이버 보안을 반드시 포함시켜야 합니다. 그리고 리더십 팀이 보안 전문 지식을 갖추도록 해야 합니다.
2. 잊지 말고 백업 생성 및 네트워크 세그멘테이션에 예산과 리소스를 집중적으로 투입해야 합니다.
3. 재해나 불리한 이벤트(랜섬웨어 공격 등)에 앞서 대응 계획을 수립해야 합니다. 조직화와 대비로 더욱 빠르고 효율적으로 대응할 수 있습니다.
4. 새로운 제품과 서비스를 통합, 설계, 개발할 때마다 보안에 미치는 영향을 분석해야 합니다. '공격자를 위한 새로운 문을 열고 있는 건 아닌가?'라고 자문해보세요.

랜섬웨어 탐지 체크리스트

네트워크에서 무슨 일이 일어나고 있을까요?

귀사가 대다수의 타사와 유사하다면 랜섬웨어 탐지는 매우 어려울 수 있습니다. 유감스럽게도 이는 귀사의 네트워크가 공격에 취약하다는 것을 의미합니다. 강력한 탐지 기능이 없다면, 금품 요구 메시지를 수신한 뒤 문제를 해결하기엔 너무 늦습니다.네트워크의 대부분이 동시에 암호화될 것입니다.

Akamai

탐지와 관련하여 랜섬웨어가 확산하는 동안 잡아내야 합니다. 필요한 것은 다음과 같습니다.

강력한 가시성

네트워크에서 무슨 일이 일어나고 있는지 모르면 랜섬웨어나 기타 사이버 위협을 탐지할 수 없습니다.

세그멘테이션 정책

일단 모든 통신이 정의되고 설명되면, 정상이 아닌 모든 것이 표면으로 떠오르고 알림을 받게 됩니다.

IDS 시스템 및 멀웨어 탐지 툴

이 툴은 알려진 취약점이나 악용에 대해 사전 정의된 룰과 시그니처를 사용하거나 보다 일반적인 또는 자동화된 비정상 탐지로 랜섬웨어 운영자의 전파 시도를 탐지합니다.

디셉션 툴

무단 측면 이동을 탐지할 수 있는 미끼, 허니팟, 분산 디셉션 플랫폼을 설정하면 정확도 높은 인시던트로 진행 중인 능동적인 유출을 효과적으로 발견할 수 있습니다.

랜섬웨어 방어 전략 구축

최고의 경계 방어에도 불구하고 보안 침해는 피할 수 없습니다. 따라서 공격의 효과를 최소화하고 네트워크 내의 확산을 막는 방어 전략을 마련해야 합니다. East-West 데이터센터 트래픽의 위협을 탐지하고 측면 이동을 차단하는 포괄적인 보안 솔루션을 제공하는 벤더를 찾으세요.

준비

IT 환경에서 실행되는 모든 애플리케이션과 자산을 식별할 수 있는 솔루션을 찾으세요. 이러한 수준의 정밀한 가시성을 통해 중요한 자산, 데이터, 백업을 신속하게 매핑하고 취약점과 리스크를 탐지할 수 있습니다. 네트워크 환경을 완벽하게 파악하면 유출 발생 시 신속하게 룰을 활성화하고 대응할 수 있습니다.

방지

솔루션을 통해 일반적인 랜섬웨어 전파 기법을 차단하는 룰을 생성할 수 있어야 합니다. 소프트웨어정의세그멘테이션을 이용하면 중요한 애플리케이션, 백업, 파일 서버, 데이터베이스 주변에 제로 트러스트 마이크로 경계를 생성할 수 있습니다. 아울러 사용자, 애플리케이션, 디바이스 간의 트래픽을 제한하고 결과적으로 측면 이동 시도를 차단하는 세그멘테이션 정책도 생성할 수 있습니다.

탐지

세그먼트화된 애플리케이션 및 백업에 대한 접속 권한을 얻으려는 모든 시도를 알려주는 솔루션을 도입하세요. 이렇게 차단된 접속 시도는 측면 이동을 나타내주는 지표입니다. 또한 알려진악성도메인과프로세스가 있음을알려주는평판기반탐지를 포함시켜야 합니다. 경계를 성공적으로 침해한 공격을 신속하게 발견함으로써 공격자들이 도착 지점을 지나기 전에 드웰 타임(Dwell Time)을 최소화하고 공격자들을 탐지할 수 있습니다.

조치

공격을 탐지하면 위협 차단 및 격리 조치의 자동 개시가 매우 중요합니다. 세그멘테이션 정책으로 중요한 애플리케이션 및 시스템 백업에 대한 접속을 차단하는 동안, 영향을 받는 네트워크 영역을 신속하게 분리할 수 있는 격리 규칙을 적용해야 합니다.

복구

마지막으로 네트워크의 여러 영역이 안전한 상태로 확인되면 연결을 점진적으로 복원하는 단계별 복구 전략을 지원하는 시각화 기능이 필요합니다.

결론

핵심 내용

기존 방어 전략을 확신하고 계신가요?

랜섬웨어는 사라지지 않을 것입니다. 실제로 2021년에 랜섬웨어는 66%의 기업에 영향을 미치면서 2020년에 비해 78% 증가했습니다. 게다가 이 수치는 감소할 조짐을 보이지 않습다. 따라서 전 세계적으로 공격 빈도 증가, 대규모의 가치 높은 표적, 랜섬 요구액 증가를 지속적으로 경험할 것이며, 이 모든 것은 비즈니스에 끔찍한 영향을 줄 것입니다. 이제 그 어느 때보다 경계에만 적용되는 접근 방식을 넘어서는 사전 계획 및 리스크 방어 전략이 필요합니다.

네트워크에서 랜섬웨어의 측면 이동을 막으세요. Akamai가 그 방법을 보여드리겠습니다.

자세한 내용을 확인하려면 **akamai.com/guardicore**를 방문하시기 바랍니다.