DELL Technologies

랜섬웨어 공격의 교훈

Universitat Autònoma de Barcelona

Gonçal Badenes
Universitat Autònoma de Barcelona의 CIO.
명확한 이해를 위해 요약 및 편집된 인터뷰입니다.

랜섬웨어 공격에 대한 대학의 대응에서는 신속한 조치, 투명성 그리고 사이버 보안 업데이트에 대한 새로운 노력이 돋보였습니다.

Dell Technologies 사이버 보안 마케팅 담당 Sameer Shah 씨가 CIO인 Gonçal Badenes 씨와 이 사건에 대해 대화를 나눴습니다.

Shah: 지금까지 조직이 사이버 보안 성숙도를 점진적으로 개선하도록 지원해야 할 필요성에 대해 이야기했습니다. 학교가 얼마 전에 사이버 공격을 받으셨죠. 공격에 대한 이야기를 자세히 나누기 전에 대학교와 IT 환경에 대해 간략하게 말씀해 주시겠습니까?

Badenes: Universitat Autònoma de Barcelona는 스페인의 주요 대학 중 하나입니다. IT 팀에서 대학을 운영하는 데 필요한 모든 서비스를 감독하죠.

공격 직전에 저희 팀은 사이버 보안 태세를 개선하기 위한 전체적인 계획을 세웠습니다. MFA(Multi-Factor Authentication)를 배포했지만 모든 서비스와 사용자 전체에 배포하지는 않았습니다. 학생과 모든 IT 직원이 이미 MFA를 사용하고 있었는데, Microsoft 365 플랫폼에서 사용할 뿐이었고 다른 서비스는 보호되지 않았습니다. 나중에 살펴보겠지만, MFA가 보편적으로 적용되지 않았던 점이 주요하게 작용했습니다.

공격은 언제 발생했으며 어떤 종류였습니까?

랜섬웨어 공격이 흔히 그렇듯 주말이 포함된 연휴에 발생했습니다. 새벽 4시경에 서비스가 도미노처럼 순차적으로 다운되고 있다는 팀원의 전화를 받았습니다. 경보가 울렸고 이러한 케이스를 예상했던 저희는 즉시 대응 팀을 구성했습니다.

랜섬웨어 공격이라는 것을 어떻게 알았습니까? 몸값을 요구하는 메모가 있었나요?

영향을 받은 시스템에 몸값을 요구하는 메모가 있었습니다. 공격자들은 주말 동안 온라인 상태였던 컴퓨터를 암호화하는 스크립트를 실행하여 소규모 공격도 감행했습니다. 그 영향은 제한적이었는데, 주요 목적은 IT 팀뿐만 아니라 직원과 학생들도 공격에 대해 알게끔 하는 것이었습니다.

그 당시 몸값 지불을 고려하셨습니까?

아니요.

그 이유는 무엇인가요?

윤리적인 입장에서 그렇게 할 수는 없었습니다. 다행히 백업이 마련되어 있었습니다. 캠퍼스 내 두 곳의 서로 다른 데이터 센터에 두 개의 복제본이 있고, 세 번째 복제본은 캠퍼스 부지 외부의 테이프에 있습니다.

명확히 하자면, 이러한 백업이 데이터 볼트(vault)는 아니었던 거죠?

예, 아닙니다. 당시에는 볼트가 없었어요. 로드맵에서 미래의 우선순위였습니다. 물론, [공격 후에는] 우선적으로 고려되었지요.

이러한 상황에서는 커뮤니케이션이 매우 중요할 수 있죠. 언론 등과 명확하고 투명하게 소통하면서 공격에 정면으로 맞선 것처럼 보입니다.

예, 첫날부터 그랬습니다. 완전히 투명하고 최대한 열린 자세로 발생한 상황을 설명해야 했습니다. 다른 사람들이 저희의 경험을 통해 대비하고 교훈을 얻을 수 있도록 노력했습니다. 일부 언론이 실제로 몸값 요구 메모를 읽고 공격자에게 연락한 것은 저희가 그러지 않았기 때문이라고 생각합니다. 공격자 그룹은 PISA(Protect Your System, Amigo) 그룹이라고 자칭하더군요.

약점이나 문제 해결 전술을 노출시키지 않기 위해 비밀을 선호하는 조직이 많습니다. 이 부분이 문제였나요?

이것은 매우 타당한 우려 사항입니다. 하지만 저는 저희 모두가 취약하다는 사실을 알고 있다고 확신합니다. 집을 안전하게 지키려고 할 때에 최대한 좋은 문을 구매하더라도 강도가 실제로 침입하려 든다면 문을 부수거나 침입할 수 있는 다른 방법을 찾을 것입니다. 이것과 완전히 똑같은 상황입니다.

저희가 공격을 받았고 취약성이 있다는 사실이 부끄럽지는 않습니다. 보호를 위한 매우 명확한 로드맵이 마련되어 있었음에도 불구하고 타격을 입었다는 사실을 사람들과 공유하는 것이 중요합니다. 훌륭한 보호 조치를 마련해 두었는데도 공격받을 수 있는 취약성이 있었습니다. 추가적인 단계를 실행하면 훨씬 더 강력한 위치를 점할 수 있습니다.

문제 해결을 시작하기 위해 즉각적으로 취한 조치가 무엇이었는지 말씀해 주십시오.

네트워크와 모든 시스템을 종료했습니다. 경찰과 지역 당국에 데이터 보호를 요청했고, 이것은 법적으로 해야 하는 조치였습니다. 그리고 곧바로 두 팀, 즉 포렌식 팀과 복구 팀을 출범시켰습니다. Dell에 전화를 걸자 이 문제는 즉시 최우선 순위로 에스컬레이션되었고, 정말 유능한 팀이 쉬지 않고 문제를 해결해 주었습니다. 이들은 보조 Data Domain에서 모든 데이터를 완벽하게 복구해냈습니다.

복구 과정에서 포렌식이 시작되었나요?

일부 복구 프로세스는 조금 기다려야 했습니다. 그래서 포렌식이 먼저 시작되었습니다. 무슨 일이 일어났는지 파악해야 했기에 모든 것이 격리되었습니다. 상황이 다시 정상적으로 돌아갈 수 있도록 다른 시스템을 만들어야 했습니다. 시간이 좀 더 걸리더라도 온라인 상태가 되는 모든 시스템이 최고의 보안 표준에 부합해야 한다고 판단했습니다.

"가장 중요한 고려 사항은 조만간 사이버 공격을 당할 가능성이 높으니 상세한 문제 해결 및 복구 계획을 마련해야 한다는 것입니다."

MFA가 Microsoft 365에만 적용되었다고 말씀하셨는데, 이것이 공격을 가능하게 한 원인 중 하나였죠. 지금은 MFA가 전체적으로 사용되고 있습니까?

사실 공격 벡터는 이미 Microsoft에 MFA를 사용하고 있는 팀원 중 자격 증명이 유출된 사용자였습니다. 공격자는 이메일 액세스를 시도했으나 MFA 때문에 액세스할 수 없다는 것을 알게 되자 검색을 계속했습니다. 그리고 마침내 MFA로 보호되지 않는 VPN이 있음을 발견했습니다. VPN을 통해 액세스한 후 네트워크를 조사하기 시작할 수 있었습니다.

저희 학교와 같이 매우 큰 네트워크에 들어온 공격자는 취약성이 있는 시스템을 찾고 측면 이동을 시작했습니다. 그래서 이제 시스템 복구를 시작한 후에는 MFA로 보호되기 전까지 무엇도 온라인에 두지 않기로 결정했습니다.

랜섬웨어 공격을 피하기 위한 주요 권장 사항이나 조언이 한 가지 있다면 어떤 것이 있을까요?

한 가지만 꼽는 것은 매우 어렵지만, 가장 중요한 고려 사항은 조만간 사이버 공격을 당할 가능성이 높으니 상세한 문제 해결 및 복구 계획을 마련해야 한다는 것입니다.

예를 들어, 포렌식 및 복구 관련 주요 파트너의 연락처를 확보하고, 복구 일정을 비롯한 상세하고 우선순위가 지정된 서비스 맵을 마련하며, 커뮤니케이션(내부 및 외부 모두)을 포함하여 주요 사업부와 잘 조율된 전략을 수립하는 것이 매우 중요합니다. 물론 공격자가 사용하는 기법에 대해 사용자가 경계하고 교육을 받도록 하는 것도 매우 중요하고요.

대학의 사이버 보안 역량이 강화됨으로써 업무를 이어 나가고 현재 하고 계신 모든 작업을 수행하는 데 대한 자신감이 높아졌다고 생각하시나요?

물론입니다. 공격 전에는 시스템을 보호하기 위한 새로운 조치가 나오면 수많은 의문과 함께 정말 필요한 것인지에 대한 우려가 제기된다는 인식이 있었습니다. 사실상 보호 조치는 절대적으로 필요합니다. 이것이 없으면 조직 전체가 위험해질 수 있기 때문입니다. 물론 이와 같은 조치로 인해 업무가 불편해진다고 생각하는 사람들도 여전히 있습니다. 하지만 대부분은 시스템이 훨씬 더 잘 보호된다고 생각합니다.

감사합니다. 보여주신 솔직하고 투명한 태도는 사이버 보안 성숙도를 향상하려고 노력하는 모든 사람들에게 귀감이 될 것입니다.