2021년 데이터 보안 전망

제로 트러스트, 비싱(vishing),
급속히 진화하는 혼란스러운
환경에 대한 전략적 접근

splunk>

갈수록 어려워지는 보안

2020년은 IT 보안팀에게 전례 없는 도전의 한 해였습니다.

기술은 빠르게 바뀌며, 조직의 공격 노출면(attack surface)이 계속해서 새로운 형태로 확장되고 있습니다. IT 보안팀은 이상 탐지를 위한 여러 도구를 보유하고 있으며 너무 많은 알람 속에 허우적대고 있습니다. 탐욕, 정치적 아젠다, 장난 등의 동기로 신종 수법을 시도하는 적들로 인해 공격 경로는 끊임 없이 변화합니다.

설상가상으로 여기에 코로나 바이러스가 추가되었습니다. 비즈니스가 아예 중단된 경우도 있고, 사무실 운영이 축소된 경우도 있습니다. 재택 근무로 인해 많은 직원들이 개인 전자 기기로 기업 네트워크에 로그인하고 기존 디지털 협업 도구에 과부하가 걸렸습니다. 검증되지 않은 새로운 방식을 사용하기도 합니다. 가장 큰 보안 위험은 정상(또는 합법)이 아닌 이메일을 분간하지 못하는 사람입니다. 그리고 지난 3월 초부터 '정상(normal)'에 대한 기능적 정의 자체가 무의미해졌다는 점도 생각해야 할 것 입니다.

이러한 상황이 적어도 2021년 말까지 이어질 것입니다.

IT 조직 전반에서 목격한 바와 같이 COVID-19 팬데믹의 엄청난 혼란이 디지털 트랜스포메이션을 가속화했습니다. 이로 인해 조직에 무질서와 부담이 가중된 상황에서 새로운 기술, 새로운 프로세스가 그 어느 때보다 빠른 속도로 도입되고 있습니다. 또한 재택 근무로 인해 기업 네트워크 보안의 상당 부분이 무력화되었습니다. Splunk CISO Yassir Abousselham은 이것이 보안팀에 막대한 부담을 안겨주고 있다고 말합니다.

"사무실, 집, 커피숍, 핫스팟 등 어디서든 위치에 관계 없이 직원들과 비정규직 인력 모두에게 동일한 수준의 보안을 제공해야 합니다." 그는 이렇게 강조합니다.

이는 실로 어려운 일입니다. Abousselham은 이러한 과제를 해결하기 위해 CISO들의 관심이 엔드포인트 보안과 제로 트러스트 보안 모델에 집중될 것이라고 말합니다.

2021년 보안 전망과 생존 전략

05
팬데믹으로 인한 근무 환경 변화가 엔드포인트 보안과 제로 트러스트 모델에 대한 관심을 가중시킬 것

07
공급망(Supply chain) 공격: 해킹 대상이 조직과 연결된 공급망 전반으로 확대될 것

09
COVID와 원격 근무를 악용한 공격: 더욱 교묘한 피싱 이메일과 기타 사기 수법 등장. 피싱이 비싱(vishing)으로 진화

12
디지털 트랜스포메이션이 급속히 진행되고 SOC에서 인공지능(AI)이 더 많이 활용될 것

14
적대적 머신러닝(adversarial learning)에 대한 방어가 향후 수 년 간 개선될 것. 왜냐하면 그래야 하기 때문.

15
2단계 인증 보편화

17
팬데믹으로 인한 혼란을 노리는 공격: 새로 도입된 기술과 불완전한 M&A의 틈새를 노린 공격이 증가할 것

19
새로운 원격 근무 패러다임 사용으로 보안 인력 부족 완화

21
계속되는 위협: 2021년에도 비슷한 상황이 이어질 것

전망

팬데믹으로 인한 근무 환경 변화가 엔드포인트 보안과 제로 트러스트 모델에 대한 관심을 가중시킬 것

IT 보안의 기초는 네트워크 보안입니다. SOC는 네트워크 경계 보호를 통해 네트워크 내의 데이터를 보호합니다. 그러나 견고하고 안전한 성벽에 대한 믿음은 무너졌습니다. 특히 직원이 실수로 문을 열 수 있다면 더욱 그러합니다. 언젠가는 공격자가 방어를 뚫고 들어오는 것이 자명합니다.

제로 트러스트(Zero trust)는 데이터를 안전하게 지키는 데 있어서 네트워크 보호에 의존하지 않습니다. 그 대신에 엔드포인트와 백엔드 애플리케이션을 보호합니다. 이 경우 네트워크 보안은 1차 방어선이 아닌 2차 방어선이 됩니다. 제로 트러스트 개념은 2019년에 보편화되었지만 COVID 시대에 원격 근무가 급증하면서 더욱 스마트한 접근방식으로 받아들여지고 있습니다.

스플렁크 보안 자문 Mick Baccio는 다음과 같이 말합니다. “제로 트러스트 방식이 계속 유지될 것입니다. 제로 트러스트는 결국 지속적인 검증이라는 오랜 원칙입니다. 이것은 사라지지 않습니다. 세상이 변하고 업무 환경이 변화함에 따라 가시성이 문제가 됩니다.”

제로 트러스트 전략은 IT 매니지드 디바이스(IT-managed device: IT부서에 의해 관리되는 디바이스)에 대한 직원들의 액세스, 각 직원의 액세스 수준과 범위 그리고 민감한 데이터에 액세스할 수 있는 기기를 감독하는 것입니다.

즉, 사무실에서 승인된 회사 노트북으로는 직원에게 액세스가 허용된 모든 데이터와 애플리케이션을 사용할 수 있지만 개인 기기로는 이메일과 채팅만 가능합니다. 올바른 엔드포인트 정책을 통해 네트워크와 관계없이 보안을 구현하고 승인되지 않은 보안이 취약한 기기에서 데이터가 유출되는 위험을 줄일 수 있습니다.

제로 트러스트 방식은 네트워크 내부의 기기들을 암묵적으로 신뢰하는 기존 경계 보안을 모든 기기, 사용자, 애플리케이션, 세션에 검증을 요구하는 방식으로 전환합니다. 하지만 이것이 기존 네트워크 보안 체제보다 더 간단합니다. Gartner는 2019년에 발표한 보고서에서 2023년까지 전체 기업의 60%가 VPN(virtual private networks)에서 제로 트러스트 이니셔티브로 전환할 것이라고 전망했습니다. 스플렁크 CISO는 코로나바이러스 팬데믹이 이러한 전환을 가속화할 것이라고 말합니다.

"엔드포인트 보안은 COVID 시대에 필수적입니다." Abousselha는 말합니다. "사무실 인력을 하룻밤 사이에 100% 원격 근무로 전환한 조직들도 있습니다. 이처럼 갑작스러운 변화가 조직의 VPN 인프라에 막대한 부하를 가져왔습니다. 이것이 비즈니스에 SPOF (single point of failure)가 되면서 조직은 시스템 가용성 위험을 줄이기 위해 클라우드 도입에 박차를 가하게 되었습니다. 이처럼 비즈니스 시스템에 액세스하는 방식이 달라지면서 새로운 보안 문제가 야기되는데, 이를 해결하는 데 도움이 되는 것이 바로 제로 트러스트 방식입니다."

"엔드포인트 보안은 COVID 시대에 필수적입니다."

Yassir Abousselham, CIO, Splunk

전망

공급망 공격: 해킹 대상이 조직과 연결된 공급망 전반으로 확대될 것

"지난 6월 Huawei가 디스플레이 아래 카메라가 숨겨져 있는 새 휴대폰의 특허를 받았다는 기사가 있었습니다. 개발 중인 어떤 신기술이든지 보안 문제를 야기할 수 있습니다." 백악관과 미국 보건복지부에 근무한 경력이 있는 보안 베테랑인 Mick Baccio는 말합니다. "국가 차원의 해킹집단이 소비자 제품에서 해당 기술을 활용하려고 했을 가능성이 높습니다. 보안이 취약한 센서들이 해킹과 멀웨어에 이용된 초기 IoT와 비슷한 경우입니다."

그는 지식 노동자들이 온갖 개인 기기와 회사 제공 하드웨어, 소프트웨어를 사용하여 집에서 로그인하는 상황이 이어지면서 위험이 증가하고 있다고 말합니다.

"현재 웹캠 물량이 부족한 상황입니다. 재택 근무와 온라인 수업 때문에 웹캠을 구매하는 사람들이 많아졌기 때문입니다. 이렇다 보니 모조품, 저가품을 구매하는 사용자들이 있는데, 이런 것들이 공격자의 눈에 들어오는 새로운 공격 경로가 됩니다." Baccio는 말합니다. "공급망 취약성은 매우 현실적인 문제입니다. 악당은 당신을 공격하는 것이 아니라 당신의 공급망을 공격합니다. 온라인에서 주문한 웹캠이나 당신이 사용하는 소프트웨어 플랫폼이 바로 그러한 통로가 될 수 있습니다."

Baccio는 이에 대한 솔루션은 내부 경계이며, 벤더들이 보안에 면밀한 주의를 기울이도록 하는 것이라고 말합니다.

"기업은 자사의 벤더 공급망을 명확하게 파악하도록 노력해야 하는데, 이는 매우 어려운 일입니다." 그는 말합니다. "내가 만약 어떤 벤더나 리셀러로부터 하드웨어나 소프트웨어 등을 구입한다면, 그 리셀러는 그 물건을 누구에게서 구입한 것일까요? 만약 물건에 보안 문제가 있다면 벤더는 어떻게 대응할까요? 계약서에 서명하기 전에 해당 벤더에 대해 조사하는 것은 실로 큰 일입니다."

“

기업은 자사의 벤더 공급망을 명확하게 파악하도록 노력해야 하는데, 이는 매우 어려운 일 입니다.”

Mick Baccio, 보안 자문, Splunk

공급망 보안을 위해서는 많은 노력이 필요합니다. 보안팀과 IT팀이 이러한 작업을 수행할 수 있을 것입니다. 하지만 보안 담당자와 IT 담당자의 노력만으로는 부족합니다. 재택 근무 환경에서 일하는 직원들에 대한 교육 또한 반드시 병행되어야 합니다. 직원이 집에서 사용할 웹캠을 구매하는데 무엇을 사라고 정확히 지시하는 것은 불가능합니다.”

“보안 인식 태도 측면에서 사람들에게 조언할 수 있습니다.” Baccio는 말합니다. “직원들의 보안 인식을 강화해야 합니다.”

내부적으로는 엔드포인트 탐지가 필수적이라고 그는 말합니다. “지금처럼 원격 사용자가 증가한 상황에서 우리는 더 많은 엔드포인트, 더 많은 하드웨어 드라이버, 홈 라우터를 모니터링해야 합니다. 이 모든 것들이 공격 경로를 증가시키기 때문입니다.” Baccio는 말합니다. “이러한 주변기기들을 모두 제로 트러스트 모델에 통합해야 합니다.”

전망

COVID와 재택 근무를 악용한 공격: 더욱 교묘한 피싱 이메일과 기타 사기 수법 등장. 피싱이 비싱(vishing)으로 진화.

피싱과 사회 공학(social engineering)에 대한 논의가 케케묵은 것처럼 느껴질 수 있습니다. 다이얼 접속 시절부터 있었던 이 오랜 문제는 사람들이 두뇌에 칩을 이식하는 시절이 오더라도 여전히 문제가 될 것입니다. 작년에는 과소평가된 사회 공학의 위험이 주목을 받았으며, 2020년을 가득 채운 충격적인 사건들 속에서도 사회 공학의 기세는 누그러들지 않았습니다.

지난 7월 Blue Check Twitter 해킹에서는 Elon Musk, Barack Obama, Kim Kardashian과 같은 유명인들의 공식 계정이 트위터 사용자들을 대상으로 한 120,000 달러 상당의 비트코인 사기에 사용되었습니다. 보고서에 따르면 이 사기는 어느 십대 청소년이 스피어피싱 기법을 사용하여 설계한 것이었습니다.지난 1월에는 'Shark Tank'라는 TV쇼의 판정단 회계 담당자가 가짜 이메일에 속아 거의 400,000 달러를 사기당했습니다.

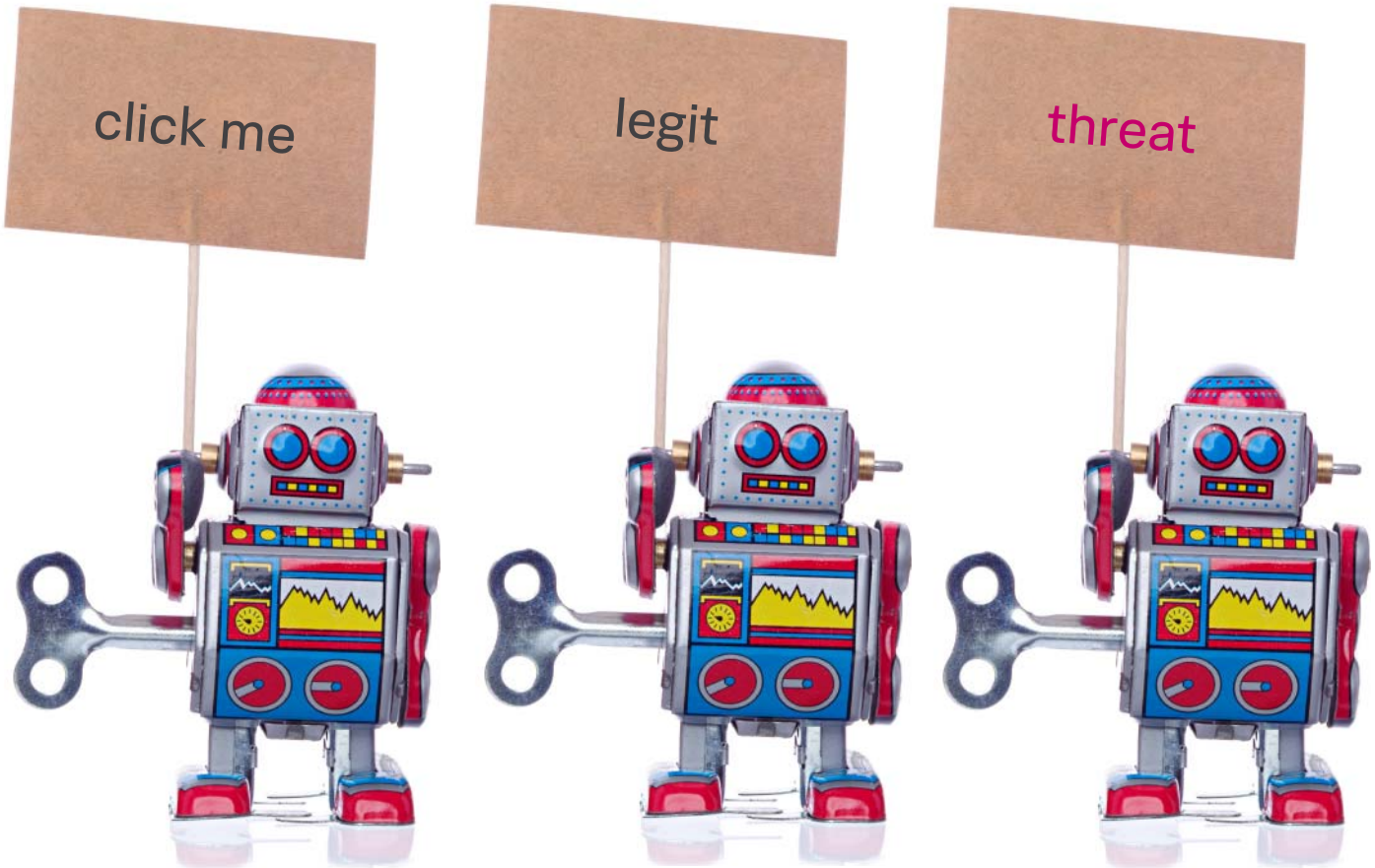
그렇기 때문에 우리 모두가 사회 공학, 특히 피싱에 대해 계속 되풀이해서 이야기할 수 밖에 없는 것입니다.

사회 공학 공격은 직원들을 속여 정상적인 것처럼 보이지만 실제로는 속임수인 행위로 유도합니다. 사기 이메일을 주의하도록 직원들을 교육하지만, 아무 것도 정상적으로 느껴지지 않고 날마다 상황이 변하는 요즘 같은 시절에는 무엇이 정상이고 무엇이 불법인지를 판단하기가 더욱 어렵습니다.

"공격자들의 전술은 동일하나 테마는 변화할 것입니다." Abousselham은 말합니다. "원격 근무 시대의 방어는 달라질 것입니다. 왜냐하면 과거에는 노트북, 워크스테이션과 네트워크 모두에 적용된 보안 컨트롤에 의존했기 때문입니다. 지금은 직원들이 원격 근무를 하므로 노트북이 기본 보안 장치이며 백엔드 모니터링과 안티피싱 솔루션이 보조적 보안을 수행합니다."

보안 자문 Mick Baccio는 새롭게 등장한 수법에 대해 말합니다. "최근 '비싱(vishing)'의 심각성이 대두되고 있습니다." 원격 근무하는 직원들이 증가하면서 공격자들이 음성 통화를 사용하여 일반적으로 사무실에 있는 작업자로부터 VPN 자격증명을 빼내는 것입니다.

"피싱 이메일은 여전히 문제이며 일상적으로 대응해야 하는 작업입니다." Baccio는 말합니다. "피싱은 앞으로도 사라지지 않을 것입니다. 앞으로 점점 더 심각해지고 구체화될 것입니다."



중요한 경고: 여전히 심각한 Shadow IT 문제

Shadow IT는 마찰을 불러오고 승인되지 않은 IT 솔루션은 문제의 심각성을 가중시킵니다. 2020년의 혼란으로 인해 더 많은 마찰이 불거지고 있습니다.

"원격 근무로 인해 IT 가시성이 제한되고 관리되지 않는 엔드포인트가 증가하면서 Shadow IT 문제가 더욱 심각해지고 있습니다." 스플렁크 보안 자문 Mick Baccio는 말합니다.

개인 기기를 사용하여 조직 리소스에 액세스하는 사용자가 증가하면서 위험은 배가됩니다. 감염된 개인 기기는 기업 네트워크에 침투하는 발판이 될 수 있습니다.

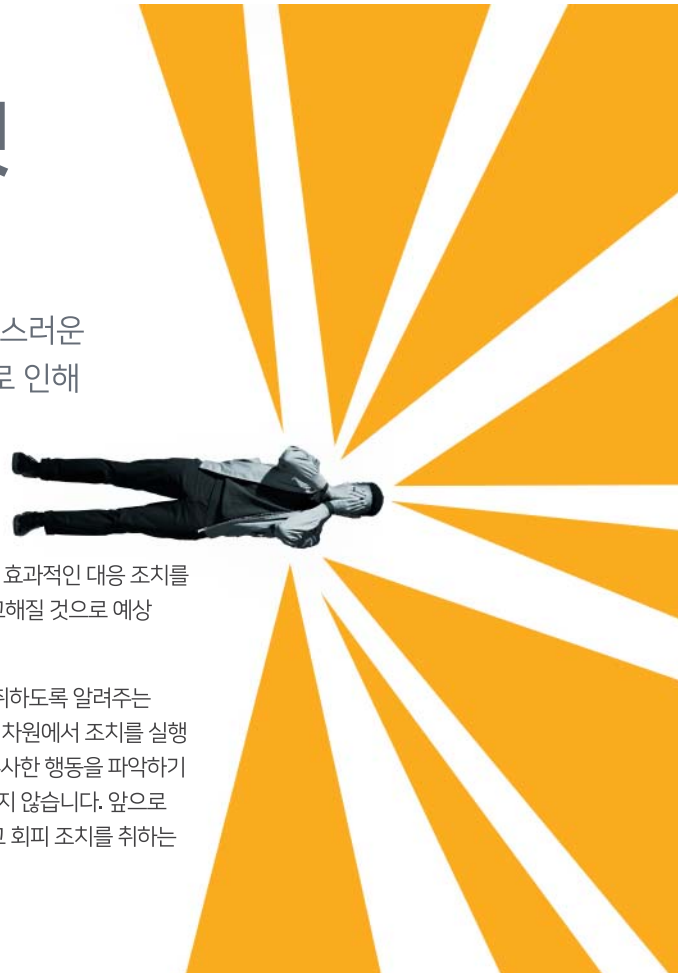
"우리는 이 문제를 해결해야 합니다." Baccio는 말합니다. "사무실이 다시 문을 열더라도 모든 직원이 복귀하지는 않을 것입니다. COVID 이후의 시대에는 원격 근무자가 더욱 증가할 것입니다. 따라서 멀웨어, 피싱, 기타 사기로부터 조직을 보호할 수 있는 더욱 강력한 가시성과 컨트롤이 필요합니다.

스플렁크 CISO Yassir Abousselham은 Shadow IT 위협에 대응하기 위해서는 제로 트러스트 솔루션, 엔드포인트 탐지 및 대응 기능, 백엔드 안티피싱 솔루션, 그리고 피싱과 기타 원격 근무 관련 위협에 대한 직원들의 인식을 강화하는 캠페인이 필요하다고 말합니다. 이와 동시에 보안팀은 가정용 컴퓨터, 개인 전화와 같은 보안이 취약한 개인 시스템을 통한 기업 데이터 유출의 위험성을 직원들에게 알려야 합니다.

전망

디지털 트랜스포메이션이 급속히 진행되고 SOC에서 인공지능(AI)이 더 많이 활용될 것

Enterprise Strategy Group이 발간한 6월 보고서에 따르면, 팬데믹 자체와 경제적 혼란만으로도 걱정스러운 상황에서 IT 임원 47%가 팬데믹 이후 사이버 공격이 늘었다고 답했습니다. 응답자 중 36%는 원격 근무로 인해 보안 취약성이 증가했다고 답했습니다.



셀 수 없이 쏟아지는 보안 경고와 수많은 잠재적 위협을 일일이 사람이 다 처리하기에는 너무 많습니다. 자동화와 기계학습(ML)은 이미 데이터의 바다에서 가장 긴급한 경고를 선별하여 특정 위협 프로필에 대한 즉각적인 조치를 취할 수 있도록 인간 보안 분석가를 지원하고 있습니다. VentureBeat 7월 기사에 미국 Chase 은행의 머신러닝 사용 사례가 소개되었습니다. Chase 은행은 고객 대상 마케팅 캠페인에 머신러닝을 사용할 뿐만 아니라, 알려진 위협과 최신 보안 위협을 파악하는 데에도 지도/비지도(supervised/unsupervised) 학습 머신러닝 알고리즘을 활용하고 있습니다.

스플렁크 머신러닝 책임자 Ram Sriharsha는 이상을 감지하고 효과적인 대응 조치를 자동화하는 AI/ML 보안 도구의 기능이 계속 향상되고 더욱 정교해질 것으로 예상합니다.

"단순히 측정 항목을 확인하여 사람에게 이상값에 대한 조치를 취하도록 알려주는 알고리즘을 넘어서고 있습니다." 그는 말합니다. "우리는 대규모 차원에서 조치를 실행하는 알고리즘과 자동화가 필요합니다. 보안 영역에서 새롭고 유사한 행동을 파악하기 위해서는 모델 학습 데이터가 과거의 공격자와 행위에만 국한되지 않습니다. 앞으로 트래픽, 데이터 등 현재 상황을 관찰하여 잘못된 패턴을 파악하고 회피 조치를 취하는 알고리즘이 등장할 것입니다."

Mick Baccio는 의미있고 실용적인 AI 애플리케이션이 해결책이라고 말합니다. "대부분의 조직에서 곧바로 이를 실현하기는 어려울 것입니다. AI를 본격 도입하기 전에 먼저 개선해야 할 사항이 백만 개는 될 것입니다."

그는 강력하고 혁신적인 알고리즘이 나오려면 최소한 2년은 더 있어야 한다며, 그 전에 자동화를 넘어 오케스트레이션으로 전환하는 것이 우선되어야 한다고 말합니다.

"여러 반복 작업들에 대한 자동화가 진행되고 있지만, 이제는 프로세스 오케스트레이션이 이루어져야 합니다. 즉, 피싱 이메일에 대한 분석을 자동화하고 처음부터 끝까지 전체 프로세스를 오케스트레이션하는 것이 필요합니다. 이메일이 수신되면 분석 기능을 통해 여러 지표들이 생성됩니다. 이것이 방화벽과 다른 시스템들로 전달되어 대응으로 이어집니다. 일부 반복 작업을 자동화하는 데 그치지 말고 전체적인 반복 프로세스를 오케스트레이션해야 합니다."

> "여러 반복 작업들에 대한 자동화가 진행되고 있지만, 이제는 프로세스 오케스트레이션이 이루어져야 합니다."
>
> Mick Baccio, 보안 자문, Splunk

전망

향후 수 년 내에 적대적 머신러닝(adversarial learning) 공격에 대한 방어가 개선될 것입니다. 왜냐하면 그래야 하기 때문입니다.

작년 스플렁크 전망 보고서에서 AI 사보타주(sabotage)의 위험성을 경고한 바 있습니다. AI 사보타주는 학습 데이터를 오염시켜 AI 기반 자동화의 결과를 망치는 것입니다. 작년 스플렁크 보고서에서는 자율주행 자동차가 정지 신호를 잘못 이해하도록 속이는 것을 예로 들었습니다. 지난 9월, 연구원들은 전투기 크기의 물체에 작은 스티커 하나를 부착하여 AI 처리 드론 영상에서 해당 물체를 숨길 수 있음을 발견했습니다. 데이터 속임수의 위협은 여전히 계속되고 있습니다. 오늘날의 AI는 태어난 지 일주일 밖에 안된 강아지만큼 순진하기 때문에 새로운 연구 영역에서의 도전에 맞서야 합니다.

연구원들은 전투기 크기의 물체에 작은 스티커 하나를 부착하여 AI 처리 드론 영상에서 해당 물체를 숨길 수 있음을 발견했습니다.

"머신러닝 알고리즘은 학습 데이터를 신뢰합니다." Ram Sriharsha는 말합니다. "하지만 사람들이 알고리즘을 의도적으로 속이려 한다면 어떻게 될까요? 업계에서는 적대적 공격이 존재하는 상황의 학습 방법에 대한 면밀한 고려가 아직 이루어지지 않았습니다."

그는 적들에 맞서 모델을 강화하는 방법에 대한 연구가 이루어져야 할 것이라고 말합니다. 그는 지금이 바로 이러한 기술을 개발할 때라고 말합니다. 왜냐하면 시장이 표준화되면 공격의 위협이 더욱 커질 것이기 때문입니다.

"수백 개의 스타트업들이 수백 가지 머신러닝 플랫폼을 파는 상황이 조만간 종식될 것입니다." Sriharsha는 말합니다. "소수, 아니면 단 하나만이 남게 될 것입니다."

그 다음에는 Microsoft 운영 체제가 시장을 지배하면서 해커들에게 거대한 단일 타겟이 된 것과 마찬가지로, 소수의 지배적인 AI 플랫폼이 모든 공격을 한 몸에 받게 될 것입니다.

"거의 모든 사람들이 사용하는 하나의 플랫폼을 중심으로 시장이 통합되면 해커들은 해당 플랫폼을 깨는 방법만 알아내면 되므로 수고를 덜게 됩니다." 그는 말합니다. "적대적인 환경에서 공격을 견딜 수 있는 강력한 알고리즘을 구축하기 위해 지금부터 많은 노력이 필요합니다."

전망
2단계 인증 보편화

예전에는 사용자가 귀찮으면 건너뛰는 선택이었던 2단계 인증이 COVID-19 덕분에 조직에서 보편적인 표준으로 자리잡을 것입니다. 2020년 사이버 범죄는 세계 경제에 매분 290만 달러의 손실을 초래하고, 이 중 약 80%가 암호와 관련된 공격이었습니다. WEF(World Economic Forum)는 작년 1월 보고서에서 암호 없는 인증(passwordless authentication)이 안전한 디지털 트랜스포메이션의 차기 혁신이라고 단언했습니다. WEF는 AI/ML 기반 행동 분석, 영지식증명(zero-knowledge proof), QR 코드 인증(이미 아태지역 국가들에서 널리 도입되고 있음)과 함께 2단계 및 생체 인증과 하드웨어 키의 역할을 강조했습니다.

그리고 COVID-19가 확산되고 갑작스럽게 재택 근무가 증가하면서 더 많은 보안 우려가 야기되었습니다. 조직의 네트워크 외부에서 로그인하는 사용자들이 증가했는데 이들 가운데 계정을 도용한 가짜가 있을 수 있기 때문입니다.

스플렁크 모바일 엔지니어링 책임자인 Jesse Chor는 보안 전문가들과 모바일 소프트웨어 엔지니어들이 이 문제로 고민하고 있다고 말합니다. "COVID와 모바일로 인해 보안 노출면(security surface)이 확장되었으며, 이것은 분명히 우려스러운 사항입니다."

방금 로그인을 시도한 것이 본인이 맞는지 확인하는 전화 앱이나 생체 스캔을 통한 2단계 인증 도입이 확대될 것입니다. 스플렁크 보안 자문 Mick Baccio는 미국 보건 복지부와 백악관에서 근무했으며, Pete Buttigieg 미국 민주당 대선 경선 후보 선거 캠프에서 CISO를 역임했습니다. 그는 다단계 인증(MFA)이 필요하다는 데 동의하며 하드웨어 토큰이 가장 유망한 솔루션이라고 말합니다. 하드웨어 토큰에는 USB 보안 키가 거의 포함되지 않으며, 휴대폰에 통합될 수 있습니다.

"하드웨어 토큰이 계정 탈취 위험을 거의 차단합니다"고 Baccio는 말합니다. "계정 탈취 위험은 보안팀의 가장 큰 골치거리 중 하나입니다. 2단계 인증으로 이러한 위험을 차단하고 다른 중요한 과제에 자원을 집중할 수 있습니다."

"지금 가장 우려스러운 점은 현존하는 모바일 운영 체제가 두 개뿐이라는 사실"이라고 Chor는 덧붙입니다. "애플이나 구글 운영 체제에 문제가 생긴다면 취약점이 얼마나 치명적일지 생각해 보십시오. 내 PIN과 관련된 단순한 버그로 인해 타인이 내 업무 네트워크에 접속하고, 내 이메일을 해킹하고, 내 전자상거래 계정을 사용하고, 내 은행 계좌를 공격할 수 있습니다. 타인이 내가 되어 모든 것을 할 수 있는 것입니다."

Chor는 2단계 인증의 폼팩터(form factor)로 생체 인식을 가장 선호한다고 말합니다. "COVID로 인해 보안과 결제를 위한 생체 인식 도입이 더욱 가속화될 것이라고 생각합니다."

생체인식 로그인의 가치는 물리적 장치를 대체한다는 것입니다. 휴대전화가 생체 인식을 위한 인터페이스라 하더라도 생체 정보가 저장되지 않으므로 도둑에게는 쓸모가 없습니다.

"이제 더 이상 무선으로 암호를 전송하지 않고 해시(hash)를 전송하는 것과 마찬가지로, 디바이스는 생체 정보의 해시를 전송할 것입니다." Chor는 말합니다. "디바이스는 클라우드에서 확인되는 정보의 통로가 됩니다. 휴대전화를 분실하거나 도난당하더라도 당신의 엄지 손가락이 손에 붙어있는 한 보안 위협은 발생하지 않습니다. 앞으로의 보안은 휴대전화가 그저 통로가 되는 방향으로 나아갈 것이라고 생각합니다."

통합에 따른 위험 증가

보안 문제는 이머징 테크놀로지 보고서에서도 다뤄집니다. 반복되는 주제 가운데 하나는 벤더 통합에 대한 우려입니다. Microsoft가 운영 체제 시장을 지배하면서 사이버 범죄자들의 주요 타겟이 되었습니다. Jesse Chor는 두 가지 주요 모바일 OS 중 어느 하나라도 결함이 생긴다면 셀 수 없이 많은 조직이 피해를 입을 수 있다고 경고했습니다. 스플렁크 머신러닝 책임자 Ram Sriharsha는 소수의 AI/ML 플랫폼 역시 해커들에게 확실한 타겟을 제공할 것이라고 말합니다.

이것은 모든 보안팀이 주시해야 하는 피할 수 없는 문제입니다.

"지금 가장 우려스러운 점은 현존하는 모바일 운영 체제가 두 개뿐이라는 사실입니다."

Jesse Chor,
모바일 엔지니어링 책임자, Splunk

전망

팬데믹으로 인한 혼란을 노리는 공격: 새로 도입된 기술과 불완전한 M&A의 틈새를 노린 공격이 증가할 것

공격자들은 빈틈을 파고듭니다. 취약점을 야기하는 두 가지 원인은 신기술 도입과 인수 합병을 통한 신규 인프라 흡수입니다. 디지털 트랜스포메이션 가속화가 전자를 증가시키고, 불황의 변동성이 후자를 심화시킵니다.

"신기술을 도입하는 IT와 해당 기술을 보호하는 보안 조직, 보안 벤더 간의 시차가 공격자에게 기회를 제공합니다." CISO Yassir Abousselham는 말합니다. "예를 들어 개발자들은 이미 Kubernetes 인프라를 구축하고 있으나 일부 보안 벤더들은 여전히 이를 솔루션에 반영하는 단계에 머물러 있습니다."

그는 클라우드 도입이 쉬워지면서 AWS, Azure, Google Cloud에서 수많은 별개의 계정들을 유지하는 관행이 위험을 초래할 수 있다고 지적합니다.

팬데믹 시대에 모두가 새로운 도전에 직면하면서 Shadow IT 성향이 증가함에 따라 보안 조직은 신기술에 특히 주의를 기울여야 합니다. (그렇다고 오래된 기술은 내버려 두라는 것이 아닙니다. 오늘날 컴퓨터 과학을 배우는 학생들에게는 신화처럼 여겨질 수 있는 COBOL 기반의 구형 정부 시스템들도 팬데믹에 따른 요구와 장애로 심각한 부담을 겪었습니다.)

또 다른 위험은 M&A로 인해 야기됩니다. 기업이 애플리케이션과 인프라를 신속하게 통합하려 하기 때문입니다. 이는 전반적인 혼란을 더욱 가중시킵니다. "인수한 회사가 선호하는 클라우드 플랫폼이 아닌 다른 플랫폼을 사용할 수 있습니다. 그렇다 하더라도 그들의 인프라를 계속 실행해야 합니다. 왜냐하면 전환이 번거로울 수 있기 때문입니다." Abousselham은 말합니다. "인수된 회사와 기존 내부 시스템 간의 신뢰 구축이 필수적입니다. 따라서 강력한 M&A 통합 프로그램이 없다면 위험이 커질 수 있습니다."

그 결과로 잘못된 구성, 보안이 불충분하거나 규정에 위배된 시스템이 초래될 수 있습니다. 이 문제를 한 번에 해결할 수 있는 솔루션은 없습니다. 조직에 도입되는 새로운 기술을 철저히 파악하고 필요에 따라 적절한 보안 수준을 보장하는 베스트 프랙티스를 수립하는 것이 중요합니다.

클라우드 보안은 새로운 스킬셋입니다.

스플렁크 보안 자문 Mick Baccio는 팬데믹 혼란으로 인해 클라우드 전환을 서두르는 조직이 흔히 맞닥뜨릴 수 있는 위험을 경고합니다. "IoT가 새로운 화두였을 때를 떠올려 보십시오. 우리는 모든 것을 인터넷에 연결하기 시작했고, 그러다가 나중에야 보안을 강화해야 한다는 것을 깨달았습니다." 그는 말합니다. "퍼블릭 클라우드 프로바이더가 뛰어난 보안 프로토콜을 사용하여 완벽한 작업을 수행합니다. 하지만 구체적인 위협 모델을 알지 못한 채 클라우드로 전환하는 사람들이 걱정스럽습니다."

그는 ITOps와 IT 보안 측면에서 클라우드 관련 스킬셋(skill sets)이 필수적이 될 것이라고 말합니다. 그는 클라우드 프로바이더의 강력한 도구가 클라우드 보안 도구 시장의 위축으로 이어질 것이며, 클라우드 프로바이더가 다양한 보안 액세스 계층을 제공할 것이라고 예측합니다. "단순히 위협 차단만을 원하십니까, 아니면 위협이 언제 어디서 어떻게 발생했는지 알기 원하십니까?"

전략

새로운 원격 근무 패러다임 사용으로 보안 인력 부족 완화

전통적으로 경영진은 직원들이 일하는 모습을 눈으로 확인하고 싶어합니다. 이 때문에 대부분의 조직이 전면적인 재택 근무 도입을 주저해 왔으나, 지역 사무소와 영업 조직을 갖춘 글로벌 조직에서는 이미 오래 전부터 다양한 형태의 재택 근무가 시행되어 왔습니다. 하지만 재택 근무 확대에는 생산성 우려 뿐만 아니라 보안 문제도 존재합니다. 그리고 유능한 인재들이 한 공간에 모여 일하고 복도나 휴게실에서 짧은 대화를 나누는 가운데 창의성과 혁신이 나온다는 실리콘밸리 격언도 있습니다.

조직은 생산성이 증가하지는 않더라도 안정적으로 유지되는 것을 확인했습니다. 그리고 리더들 또한 원격으로 직원들과 업무를 관리하는 방식에 적응했습니다.

그러나 지난 수 개월 동안 전 세계 지식 노동자들이 어쩔 수 없이 재택 근무를 해야했던 상황 속에서 조직은 생산성이 증가하지는 않더라도 안정적으로 유지되는 것을 확인했습니다. 그리고 리더들 또한 원격으로 직원들과 업무를 관리하는 방식에 적응했습니다. 스플렁크 CTO인 Tim Tully는 자신이 재택 근무에 회의적이었음을 인정하면서 팬데믹 이후 전 세계 6,000여 명 이상의 스플렁크 직원들이 성공적으로 원격 근무를 수행하고 있다고 말했습니다.

"원격 근무 직원을 더욱 확대할 것"이라고 그는 말합니다. "2년 전만 해도 저는 우리 팀이 최소한 동일한 시간대에 근무해야 한다고 말했을 것입니다. 이제는 핵심 이니셔티브를 수행할 최고의 인재를 찾을 수만 있다면 그들이 어디에 있는지는 신경 쓰지 않습니다. 그것이 바로 우리의 변화된 모델입니다."

스플렁크의 최고 인사 책임자인 Kristen Robinson은 인재 확보를 위해 더 먼 지역까지 검토하는 조직이 증가할 것이라고 말합니다. "다양한 산업 전반에서 원격 근무가 효과적으로 수행될 수 있음이 입증되었습니다. 지리적 위치에 관계없이 최고의 인재를 모집한다는 측면에서 새로운 기회가 열릴 것이라고 확신합니다."

ISO Yassir Abousselham도 여기에 동의합니다. “원격 근무자 관리에 자신감이 생기면서 현지 인력이 부족할 경우에 전 세계의 인재를 고용할 수 있게 되었습니다.”

IT 보안에서 숙련된 인력의 부족은 매우 심각합니다. 노동시장 분석업체 EMSI의 지난 7월 보고서에 따르면 미국 내 사이버보안 분석가에 대한 수요는 공급의 두 배였습니다. 이 보고서는 기존 직원의 재교육 뿐만 아니라, 원격 근무자 채용과 이들에 대한 관리 및 지원을 위한 효율적인 시스템의 도입이 도움이 될 것이라고 권고합니다.

국제 고용은 급여, 세금, 복리 후생 등과 관련된 규제 문제를 야기한다고 Abousselham은 지적합니다. 하지만 그렇다고 해서 이를 포기할 수는 없습니다. “원격 근무는 뉴노멀(new normal)입니다. 우리는 새로운 기회를 포착하기 위해 필요한 프로세스와 기능을 마련해야 합니다.” 그는 이렇게 말합니다.

노동시장 분석업체 EMSI의 지난 7월 보고서에 따르면 미국 내 사이버보안 분석가에 대한 수요는 공급의 두 배였습니다.

계속되는 위협: 2021년에도 비슷한 상황이 이어질 것

2020년의 보안 위기는 2021년에도 마찬가지로 계속될 것입니다. 보안팀은 대규모 장애의 가능성에 대비해야 합니다. 팬데믹으로 인해 모든 대륙에서 비즈니스가 중단되었습니다. 2020년 상반기에는 대형 산불이 호주를, 하반기에는 미국 서부 전체를 강타했습니다. 그 외에도 이상 기후로 인한 피해가 정기적으로 비즈니스에 장애를 초래하고 있으며, 이로 인해 CISO의 보안 프로그램에 구멍이 뚫릴 수 있습니다.

혼란이 계속되는 상황에서 가장 큰 보안 전략 두 가지는 앞서가는 조직들이 도입한 HR 전략을 반영합니다. 조직 전체의 공동 작업을 넘어 모든 개인의 복지에 관심을 가져야하는 것과 마찬가지로, 보안팀은 엔드포인트 보안에 중점을 기울여야 합니다. 그리고 모든 회의가 서로의 안부와 상황을 확인하는 것으로 시작되는 요즘 세상에서 직원/파트너와의 커뮤니케이션에 집중하여 간과될 수 있는 새로운 보안 문제를 해결하도록 지원해야 합니다.

2020년이 기록적인 해였던 것처럼, 2021년에도 엄청난 도전이 계속될 것입니다. 보안팀은 조직이 COVID 상황에서 여기까지 오는 데 중요한 역할을 수행했습니다. 이제는 다른 방향으로 나아가도록 지원할 때입니다.

주요 참여 임원

Yassir Abousselham

Yassir Abousselham은 스플렁크 CISO(chief information security officer)입니다. 이전에는 Okta와 SoFi에서 CISO로 재직한 바 있으며, Google과 EY 임원을 역임했습니다. 샌프란시스코 Evanta CISO Summit 공동 의장부터 사이버보안 스타트업 자문 역할까지 사이버보안 업계에서 활발한 활동을 펼치고 있습니다.

Kristen Robinson

CPO(chief people officer)인 Kristen Robinson은 급속히 성장하는 기업에서 혁신의 기반은 사람이라는 신념을 갖고 있습니다. 스플렁크에 입사하기 전에는 Pandora에서 최고 인사 책임자로 재직하였으며, Yahoo에서 HR 담당 SVP를 역임 했습니다.

Mick Baccio

스플렁크 보안 자문을 맡기 전에는 미국 민주당 대선 경선 후보 Pete Buttigieg의 캠프에서 CISO직을 수행했습니다. 오바마 백악관 및 보건복지부에서 사이버보안 및 위협 인텔리전스 업무를 담당했습니다. 그는 또한 전문적인 락피커(lockpicker) 입니다.

Ram Sriharsha

Ram은 스플렁크 머신러닝 책임자로서 스플렁크를 구동하는 최첨단 ML 기술의 적용을 총괄하고 있습니다. 이전에는 Databricks에서 유전체학을 위한 엔지니어링과 제품 개발을 총괄하였으며 암스테르담에서 Apache Spark의 R&D 센터 설립 멤버로 일했습니다. Yahoo Research 수석 과학자로 재직하였으며 메릴랜드 대학교에서 이론 물리학 박사 학위를 받았다.

Jesse Chor

Jesse는 스플렁크 모바일 엔지니어링 책임자입니다. 이전에는 Yahoo에서 소프트웨어 개발 엔지니어링 디렉터로 일했습니다. 그 이전에는 모바일 마케팅 스타트업 Sparq를 설립하고 CEO직을 역임했습니다. Sparq는 Yahoo에 인수되었습니다.

Tim Tully

Tim은 스플렁크 CTO(chief technology officer)이며 제품 및 기술 조직을 총괄하고 있습니다. 스플렁크에 입사하기 전에는 Yahoo에서 CDA(chief data architect), 엔지니어링 부사장 등으로 14년 간 재직했습니다. 그는 데이터, 설계, 모바일 분야의 전문가로서 기업, 스타트업, 대학에 자문을 제공하고 있습니다.

2021년 전망 보고서와 이머징 테크놀로지 및 IT 운영 보고서에서 더 많은 인사이트를 확인할 수 있습니다.

자세히 보기

20-15669-SPLK-Predictions 2021-Data Security-109

splunk>