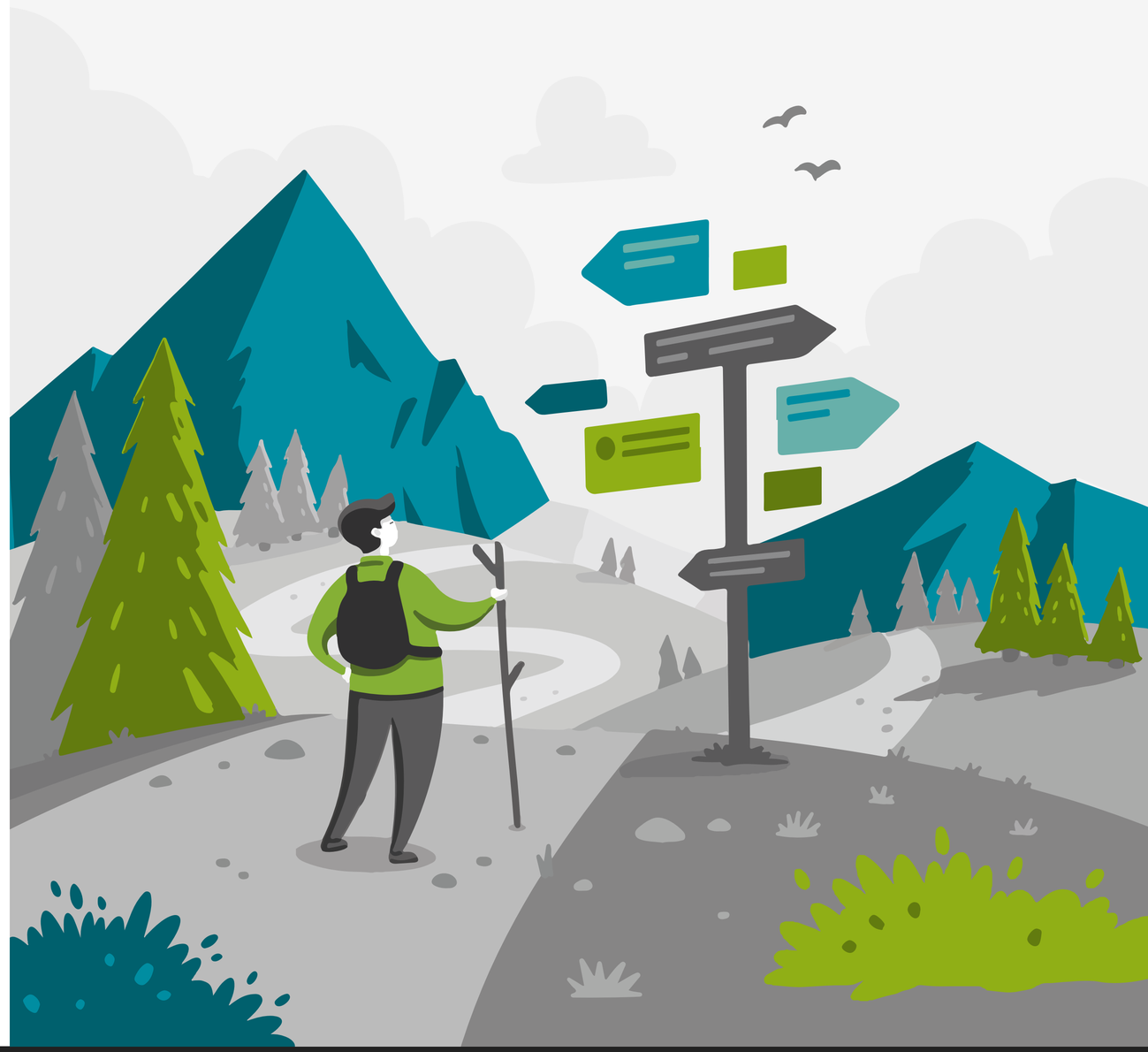
JUNIPER NETWORKS | Engineering Simplicity

eGuide

사이버 보안의 기본지식 이해하기

작성자: 트레버 포트

주니퍼 네트웍스 기술 보안 책임자



소개

본 문서는 기본 IT 인포섹 방어의 기본 요소, 그 역할과 중요한 이유를 다룹니다.

정보 보안 또는 '인포섹(infosec)'은 정보 보호에 관련된 모든 것, 즉 원칙, 도구, 테크닉, 기술, 제품, 서비스 그리고 관행에 대해 설명합니다. 인포섹은 사람과 함께 시작하고 끝납니다. 침해 사고는 거의 대부분 휴먼 에러로 인해 발생합니다.

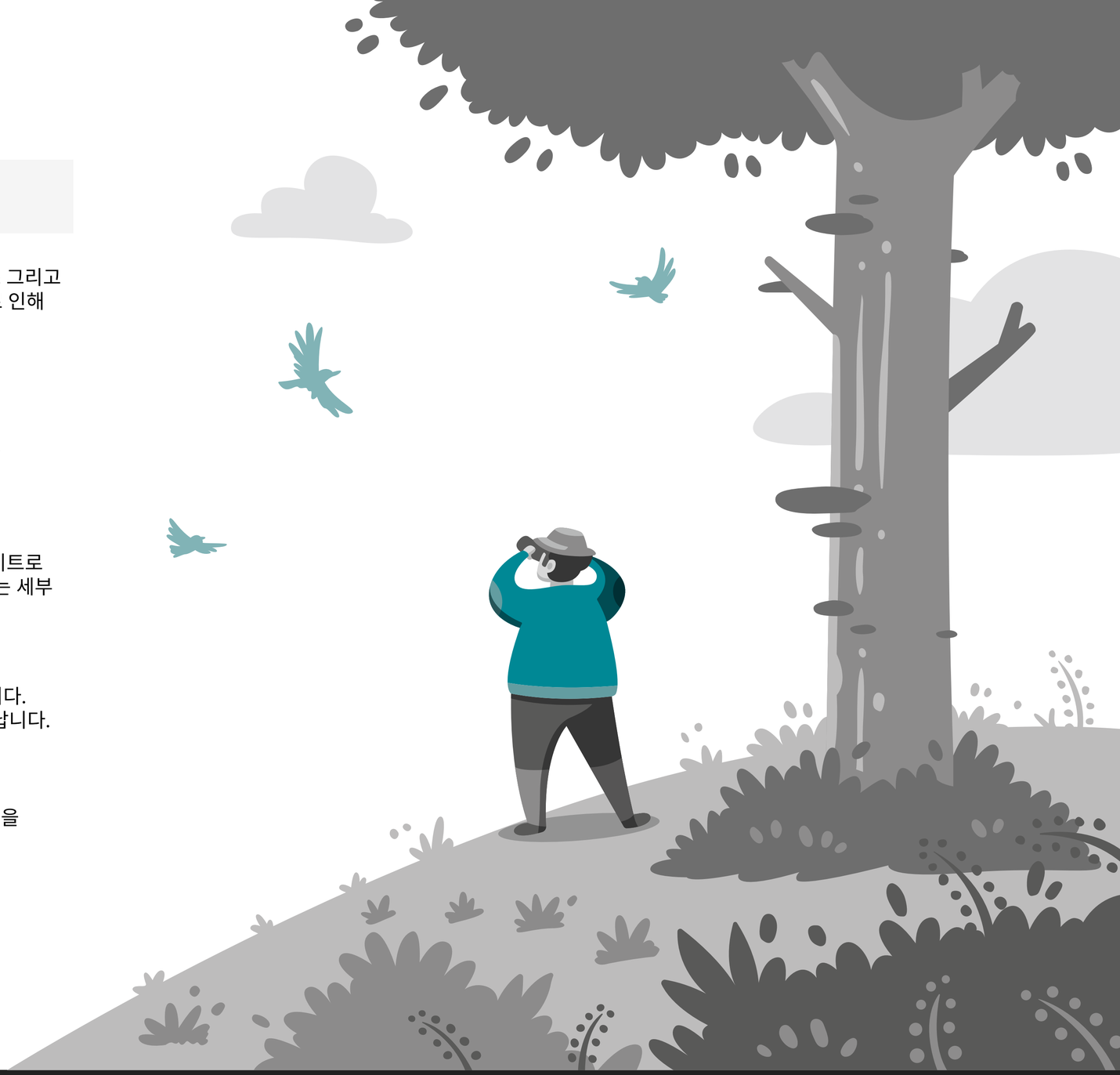
인간에 의한 침해는 **무지, 소셜 엔지니어링, 그리고 과실**이라는 세 가지 주요 범주로 나뉩니다.

무지는 지식의 결여이며, 모르는 것을 안다고 오해할 때 무지는 보안 위험이 될 수 있습니다.

소셜 엔지니어링은 소위 'Microsoft 기술자'의 가짜 전화처럼 간단할 수도 있고, 복제 웹사이트로 유도하는 스피어 피싱 이메일처럼 정교할 수도 있습니다. 그 목적은 계정에 액세스할 수 있는 세부 정보를 공개하도록 만드는 것입니다.

소셜 엔지니어링에 대해서는 우리 모두 무지하고 취약할 수 있지만, 과실은 선택의 문제입니다. 의도적으로 교육 또는 업무 수행 등 의무의 일부 측면을 고의로 방치하도록 선택할 때 일어납니다.

다행히도 기술을 사용하여 공격을 차단하고, 운영자에게 알림을 전송하고, 악의적, 비정상적, 과실적 행동을 감지함으로써 인포섹 침해 사고 방지를 지원할 수 있습니다.



기본 IT 인포섹

데이터와 메타데이터

대부분의 정보는 컴퓨터의 어딘가에 데이터로 저장되어 있습니다. 파일이나 데이터베이스뿐만 아니라 사진, 단어 문서, 기록 등으로 말입니다.

그 외에도 메타데이터라고도 알려진 정보에 대한 정보 또한 중요합니다.

사진은 종종 GPS 좌표 또는 이미지를 촬영한 디바이스의 세부 정보와 같은 메타데이터를 포함하고 있습니다. 이미지를 소셜 미디어에 게시할 때 이러한 메타데이터를 제거하지 않는다면 악의적 행위자가 이를 사용하여 대상의 위치는 물론 심지어 해당 개인을 식별하는 데 도움이 되는 핸드폰 유형까지 파악할 수 있습니다.

누군가가 음식 셀카를 찍고 이를 소셜미디어 메시지에 첨부한다고 생각해봅시다. 이 사진은 도둑에게 위치와 시간을 알려줍니다. 간단한 계산만 하면 도둑이 물건을 훔치기 전에 그 사람이 집으로 돌아갈 수 있는지를 알려줍니다.

메타데이터는 또한 기업 비밀을 드러낼 수 있습니다. 전기 담당자가 아직 발표되지 않은 데이터센터에서 방금 완료한 케이블 작업 사진을 게시하면 메타데이터를 보는 모든 사람에게 그 위치를 쉽게 누설할 수 있습니다. 마찬가지로, Word 문서는 편집한 모든 사람의 내역을 유지하는 경향이 있기 때문에 법적 결과를 초래할 수 있습니다.

방화벽과 안티멀웨어를 넘어서

전통적인 방화벽 및 안티멀웨어는 그 자체로 특별한 효과가 있지는 않습니다.

기존 방화벽은 누군가 사용자의 PC를 원격 제어하지 못하도록 막을 수 있지만, 피싱 이메일은 필터링하지 못합니다. 이러한 이메일은 클릭하면 방화벽 뒤에서 작동하거나 또는 PC에 원격 액세스를 허용하도록 방화벽을 재구성할 수 있는 원격 제어 애플리케이션이 자동으로 다운로드될 수 있습니다.

마찬가지로, 안티멀웨어 애플리케이션은 알려진 유형의 악의적 파일에 대한 방어는 잘하지만, 이전에 본 적이 없는 파일에 대한 방어에는 별로 효과가 없습니다. 따라서 인터넷 브라우저를 통해 사용자의 PC로 침입하는 무수한 침입자들을 방어하는 데는 사실상 쓸모가 없습니다.

기업에서는 대부분의 인포섹 제품 및 서비스의 초점을 인플라이트(in-flight) 데이터, 즉 이동 중인 데이터에 맞추고 있으며, 어떤 사고가 발생하든지 사용자에게 도달하거나 네트워크를 탈출하기 전에 잡아내는 것을 목표로 합니다.

차세대 인포섹

90년대에 애플리케이션과 외부 세계 사이에서 프록시 역할을 수행하는 애플리케이션 계층 방화벽을 사용하기 시작했습니다. 그리고 차세대 방화벽(Next Generation Firewalls: NGFW)이 그 뒤를 이었는데 조직 인프라에 더 많이 통합되며 IP만이 아니라 사용자 이름 또는 그룹에 기반한 정책 적용 등의 고급 기능을 제공합니다.

일반적으로 NGFW는 악의적 존재가 기본 공격을 사용하여 외부에서 네트워크로 액세스하지 못하게 방지하며, 또한 피싱 시도에 대한 이메일 스캔과 같은 일부 형태의 인플라이트 데이터 스캐닝 기능을 제공합니다. NGFW는 수천 명의 사용자를 한 번에 보호할 수 있으며, 프린터와 같이 바이러스 보호 기능을 사용할 수 없는 엔드포인트를 방어할 수 있습니다.

차세대 안티멀웨어(Next-Generation Anti-Malware: NGAM) 또는 차세대 안티바이러스(Next-Generation Anti-Virus: NGAV)는 설치된 호스트만 방어할 수 있습니다. 따라서 NGFW를 사용하여 소셜 엔지니어링 공격을 방어할 수 있습니다.

NGFW는 애초부터 악성 시도가 사용자의 PC에 도달하지 못하도록 시도하기 때문에 최상의 가장 안전한 옵션입니다.

NGAM(또는 NGAV)은 악성 시도가 사용자의 PC에 진입했을 때 침해 사고를 방지하도록 시도하는 최후 방어선입니다.

기본 IT 인포섹

WAF와 애플리케이션 보안

다음 진화 단계는 웹 방화벽(Web Application Firewall: WAF)입니다. WAF는 HTTP 및 HTTP 전달 애플리케이션에 초점을 맞춘 애플리케이션 계층 방화벽이며, 일반적으로 (네트워크 내부 또는 외부) 인터넷을 통해 액세스합니다.

WAF는 특정 애플리케이션이나 애플리케이션 등급의 특정 취약점을 보호합니다. 예를 들어, WAF는 악의적 SQL 명령을 필터로 찾아내 실행되지 않도록 방지합니다. WAF는 내부적으로 내부자 위협으로부터 보호하고, 애플리케이션의 한 계층이 보안이 침해된 다른 계층에 의해 영향받지 않도록 방지하는 데 사용되는 경우가 많습니다.

애플리케이션 보안이 방화벽, 안티멀웨어, 보안을 제공하는 다른 외부 제품 또는 서비스에 항상 의존하는 것은 아닙니다.

기존 애플리케이션 보안은 애플리케이션 자체에 직접 보호 계층을 구축합니다. PC용 안티멀웨어 애플리케이션처럼 애플리케이션 보안은 서버 기반 애플리케이션을 위한 절대적인 최종 방어선입니다. 만약 공격이 그 수준까지 진행된다면, 과정 중에 인포섹에 심각한 문제가 발생한 것입니다.

심층 방어

단일한 벤더가 오늘날의 위협으로부터 네트워크를 방어할 수는 없으며, 누구도 새로운 위협에 대응하는 혁신적인 새 접근 방식을 좇아가는 데 충분한 인력이나 연구 및 개발 능력을 갖추고 있지 않습니다.

최신 네트워크를 방어하는 유일한 현실적 방법은 긴밀하게 협력하여 다계층 심층 방어를 제공하는 다양한 벤더로부터 여러 제품을 공급받는 것입니다.

암호화와 DLP

암호화 및 데이터손실방지(Data Loss Prevention: DLP)는 네트워크 내부의 데이터가 유출되지 않도록 설계되었습니다.

암호화 기술은 올바른 키를 가지고 있는 개인 또는 애플리케이션만 데이터에 액세스할 수 있도록 보장합니다.

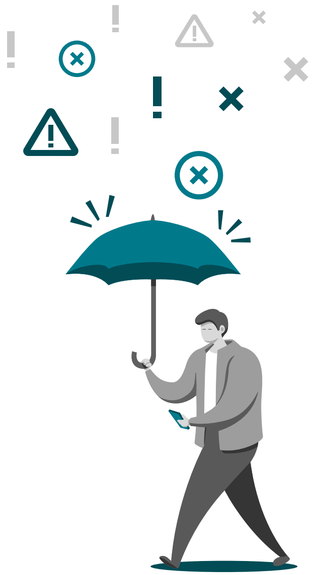
예를 들어 암호화하지 않은 고객 파일이 담긴 판매 관리자의 노트북을 도둑맞는다면 조직에 큰 손해가 발생할 수 있습니다.

인플라이트 데이터에 대한 암호화를 사용하여 제3자에 의해 데이터가 스누핑되지 않도록 합니다. 이는 인터넷 제공 서비스나 무선 네트워크를 통한 액세스 시 필수적입니다.

기본 DLP 접근 방식은 네트워크에서 벗어나려는 데이터를 스캔하며 해당 데이터가 벗어나서는 안 되는 경우에 이를 막습니다. 이러한 방식은 종종 NGFW와 NGAV로 구축되어 예를 들어, 특정 유형의 콘텐츠가 담긴 파일이 플래시 드라이브로 복사되거나 클라우드 스토리지 폴더(예: Dropbox)에 업로드되는 것을 방지합니다.

DLP는 종종 클라우드 액세스 보안 브로커(Cloud Access Security Brokers: CASB)와 고급 위협 보호(Advanced Threat Protection: ATP) 제품을 비롯한 보안 도구에 통합되어 있으며, 예를 들어 신용카드 정보가 담긴 스프레드시트의 전송을 감지하고 경고 또는 차단을 생성합니다.

하지만 네트워크에서 데이터를 몰래 빼내는 방법은 더 많습니다. 인스턴트 메시지, Slack, 소셜미디어는 최신 DLP가 잘 다루지 못하고 있습니다.



기본 IT 인포섹 방어

모니터링

모니터링을 하지 않는다면 IT 실무자는 무슨 일이 일어나고 있는지, 또는 어떤 문제에 대응해야 하는지 알 수 없을 것입니다. 대부분의 모니터링 제품은 편차와 상관관계를 사용하여 패턴을 발견합니다.

편차를 알아내는 방법은 실시간으로 시스템 간의 워크로드 및 데이터 흐름을 관찰하여 '정상' 형태의 기준을 확립한 다음, 이 기준에서 벗어난 부분을 식별하는 것입니다.

상관관계 기반 모니터링은 동시에 또는 연속으로 발생한 여러 문제 이벤트를 찾아내며, 일반적으로 애플리케이션 또는 인프라 구성 요소로 생성한 이벤트 로그를 기반으로 합니다.

이상적인 모니터링 기반 DLP 시스템은 조직의 IT 인프라 전반에 대한 데이터 액세스를 검토하여 비정상적인 요소를 찾습니다. 예를 들어, 평소 하루에 약간의 계정에 관한 정보에 액세스하는 영업 관리자가 해당 지역 내 모든 계정 정보를 갑자기 불러온다면, 시스템에서 뜻밖의 사건이 발생할 수 있음을 찾아냅니다. 이러한 접근 방식에는 협업하는 여러 벤더가 제공하는 여러 제품이 필요합니다.

그러나 모든 조직 데이터에 대한 전체 모니터링은 불가능한 경우가 많습니다. 기업은 온프레미스 및 퍼블릭 클라우드 모두에서 수천 가지의 다양한 위치 및 시스템에 데이터를 보유할 수 있습니다.

조직이 모든 데이터 액세스를 모니터링할 수 있더라도, 이것을 어떻게 해야 할지의 문제가 있습니다. 비정상적인 액세스 패턴은 데이터를 훔치려는 직원, 외부 공격자로 인해 발생하는 보안 침해 이벤트이거나 단지 해당 작업을 수행하려는 사람일 수 있습니다. 머신러닝은 이러한 패턴을 미세하게 조정하기 위해 점차 사용이 증가되고 있으며, 향후 몇 년간 상당히 발전할 것으로 보입니다.

SIEM과 ATP

SIEM(Security Information and Event Management) 제품은 인포섹 허브로 점점 더 ATP 제품과 합쳐지고 있습니다. 여러 제품에서 데이터를 수신하며 여러 벤더의 주요 제품과 빠르고 단순하게 통합되기 때문에 아주 유용합니다.

가장 성공적인 SIEM과 ATP는 상관관계에 중점을 둡니다. 예를 들어보겠습니다.

1. NGFW는 ATP로 이메일 데이터 스트림을 전송하며, 여기서 해당 사용자를 대상으로 하는 일련의 멀웨어 포함 이메일을 감지합니다.
2. ATP는 방화벽을 학습시켜 이메일이 도착하지 않도록 합니다.
3. 잠시 후에 해당 사용자 엔드포인트 상의 NGAV는 이상한 행동을 감지합니다.
4. CASB는 엔드포인트가 클라우드 스토리지 사이트에 연결하고 문서를 업로드하려는 시도를 감지합니다.

각 이벤트에 대한 경고 심각도가 낮을 경우에도 ATP가 이벤트들을 서로 관련지으면, 표적 공격이 발생 중일 수 있다고 판단하고, 최대 위협으로 선언하여 인력을 호출할 수 있습니다.

SIEM은 주로 이벤트 및 모니터링 데이터를 수집하며, 많은 벤더는 스캐닝 기능을 추가하고 DLP에 구축하거나 DLP를 갖춘 애플리케이션과 연동을 가능하게 만들기 시작했습니다.

기본 IT 인포섹 방어

액세스 제어, VPN, 그리고 원격 액세스

암호화와 같은 인포섹 기술 덕분에, 저장 장치에 물리적으로 액세스할 수 있으나 실제 데이터에는 액세스하지 않을 수 있습니다. 마찬가지로 클라우드 컴퓨팅은 조직이 기본 하드웨어에 액세스하지 않고도 세계 어디에서나 제품, 서비스 및 데이터에 액세스할 수 있게 해줍니다.

거의 모든 IT 인프라, 운영체제, 애플리케이션은 특정 형태의 액세스 제어 기능을 갖추고 있습니다. 액세스 제어 가장 중요한 방법 두 가지는 가상 사설 통신망(Virtual Private Networks: VPN) 및 원격 액세스입니다.

VPN은 컴퓨터 시스템 둘 사이의 암호화된 네트워크 터널입니다. 개인이 소속 조직의 프라이빗 네트워크에 안전하게 연결하고 사이트 간에 안전한 링크를 구축하기 위해 사용합니다. 또한 악의적 행위자의 스누핑으로부터 보호하기 위해 암호화를 사용합니다.

원격 액세스는 개인이 VPN을 사용하지 않고도 조직 리소스에 액세스하도록 허용하는 여러 기술에 사용하는 용어입니다.

브라우저 방어

이메일 외에도 웹 브라우저는 외부 공격자가 사용자 디바이스 또는 엔드포인트를 손상시키기 위해 사용할 가능성이 가장 높은 경로일 것입니다.

현재의 웹 브라우저는 여전히 매우 취약하며, 사용자가 인터넷에서 파일을 다운로드한 뒤 실행하도록 허용하는데, 이는 인포섹 침해 사고 중 세 번째로 흔한 수단입니다.

Chrome과 Firefox 같은 인기 웹 브라우저는 Adblock, Ghostery 및 Privacy Badger와 같은 확장 프로그램을 설치하는 기능을 제공합니다. 이러한 프로그램은 멀버타이징과 같은 다양한 형태의 인터넷 악성 시도로부터 보호를 제공하며, 웹 브라우저가 의심스러운 인터넷 리소스에 대한 연결 요청을 시도하지 않도록 방지하는 것을 목표합니다.

NGAV 벤더가 제공하는 기타 브라우저 확장 프로그램은 보안이 침해된 리소스에 액세스하는 요청이 완료되지 않도록 막음으로써 최종 사용자를 보호합니다.

기본 IT 인포섹 방어

MDM

모바일 디바이스 관리(Mobile Device Management: MDM) 제품은 조직 방어선의 외부에 존재하는 디바이스(휴대전화, 태블릿 및 노트북 등)를 위해 설계되었습니다. 이 제품은 원격 및 모바일 디바이스에 보안 템플릿, 프로파일 및 정책을 적용하며, 기업 방어선 너머의 리소스에 연결할 수 있기 전에 조직 인포섹 요구 사항을 충족하도록 보장합니다.

MDM은 앱스토어 및 가상 데스크톱 인프라(Virtual Desktop Infrastructure: VDI)와 같은 솔루션을 통해 보안 애플리케이션 전달 기능을 제공합니다. 또한 MDM 제품은 액세스 제어를 통해 승인된 사용자만 장치를 사용할 수 있도록 보장하며 장치를 도난당하거나 분실한 경우 추적 또는 원격 유인을 활성화합니다.

인증

중앙화된 인증 및 통합인증(Unified Authentication: UA) 기술은 LDAP, SAML, 또는 Microsoft의 Active Directory 같은 디렉터리 서비스에 의존합니다. 통합인증(Single Sign-On: SSO)은 가장 잘 알려진 UA 기술로, 사용자가 단일 사용자 이름 및 암호를 사용하여 여러 다른 인프라에 위치한 복수 프로바이더의 워크로드 및 서비스에 액세스하도록 허용하는 것이 목표입니다.

다요소 인증(Multi-Factor Authentication: MFA) 시스템도 널리 사용하지만, 국가에 따라 달라져야 하는 경우처럼 복잡성이 생길 수 있습니다. 예를 들어 SMS 인증(일반적인 MFA 접근)은 사용자가 로그인하기 위해 문자 메시지의 코드를 입력해야 하지만, 많은 국가에서 SMS 메시지를 신뢰할 수 없도록 만드는 제한을 적용하거나, 적절한 작동을 위해 추가 통합을 요구할 수 있습니다.

자동화

관리하에 있는 워크로드의 수와 다양성은 빠르게 증가하고 있습니다. IT 변화 속도는 한동안 가속화를 멈추지 않았으며, 인간은 도움 없이 이를 따라잡을 수 없습니다. 여기서 자동화가 필요합니다.

자동화는 무엇보다도 가장 중요한 인포섹 방어입니다.

최신 IT의 고도로 상호연결된 특성, 빠르게 사라지는 네트워크 방어선, 그리고 방어선 너머에서 위협이 발생할 수 있다는 사실 때문에 인포섹은 모든 IT 측면의 일부가 되어야 합니다. IT 인프라의 모든 부분, 모든 워크로드, 모든 네트워크 연결 디바이스는 조직 인포섹 설계의 일부여야 합니다.

공격 분석

목표 정의

밥이라는 해커가 있다고 해보겠습니다(여성 해커도 있지만, 통계적으로 범죄자는 남성일 가능성이 높습니다). 밥의 목표는 현지 인터넷 서비스 프로바이더인 PotatoCom입니다. PotatoCom은 여러 해 동안 연속으로 파이버-옵티컬 인터넷 설치를 거부했고, 밥은 끔찍한 ADSL에 질렸습니다. 밥은 복수를 하려고 자체 데이터베이스에 대한 액세스를 거부하여 PotatoCom 금융 시스템의 보안을 침해하려고 합니다.

시스템을 제어해서 계획 수행을 하려고 밥이 일류 기술자가 될 필요는 없으며, 다만 목표를 달성하기에 충분한 내용만 학습하면 됩니다.

연결

밥은 추적할 수 없는 방식으로 자신의 불법 온라인 활동을 수행할 방법을 찾아야 합니다. 커피숍에서 보안이 되지 않는 공공 Wi-Fi를 사용할 수 있지만, 그곳까지 가는 동안을 포함해서 감시 카메라에 나타나지 않아야 합니다. 피할 수 없는 (또는 감지하지 못한) 카메라를 통과할 경우를 대비해서 자신을 보호하기 위해 물리적 위장을 할 수 있습니다.

그는 동일한 Wi-Fi 핫스팟을 절대로 두 번 사용하지 않을 것이며, 다양한 무료 Wi-Fi 장소에 가기 위해 다양한 대중교통 유형을 이용하고 눈에 띄는 활동 패턴을 피할 것입니다. 연결에 충분할 만큼 근접할 수 있다면 무료 Wi-Fi를 제공하는 비즈니스 건물에 들어갈 필요도 없을지 모릅니다.

또한 밥은 사용하는 네트워크상의 모든 감시 기술로부터 자신의 활동을 숨겨야 합니다. 그는 아마도 한 개나 그 이상의 VPN을 사용해야 할 겁니다. 또한 공격을 실행할 장소로서 VM이나 가상 사설 서버를 임대할 수 있습니다. 자신의 인터넷 트래픽을 더 숨기기 위해서 그는 아마도 TOR, I2P 또는 다른 익명화 및 암호화 방식을 사용할 것입니다.

결제

온라인을 할 때마다 밥은 USB 플래시 드라이브, 노트북 컴퓨터, 2개의 VPN 서비스 계정과 2개의 사설 VM 렌탈을 구입해야 합니다. 따라서 그는 신원을 드러내지 않고도 이를 수행할 방법을 알아내야 합니다. 수행할 방법은 있으며, 복잡할 수 있지만 가능합니다. 간단히 말해서 밥은 현금을 선불 신용카드로 전환해서 (합법적으로) 관리하며 어디서든 사용할 수 있으며, 역추적 당하지 않습니다.

연구

밥은 PotatoCom이 어떤 데이터베이스 및 백업 시스템을 사용하는지, 그리고 해당 시스템에 어떻게 들어가는지 알아내야 합니다. 그는 PotatoCom의 IT 인프라를 조사하기 위한 기술적 수단을 사용할 수 있습니다. 소셜 엔지니어링을 사용하여 여러 PotatoCom 직원과 채팅하면서 자신을 알만한 사람(또는 내부자)으로 제시하면서 사람들에게 유출의 여지를 줄 수 있으며, 이런 방식은 보통 잘 통합니다. 또한 사용하는 도구를 잘 이해하는 PotatoCom 직원들을 검색하여 소셜 미디어에서 필요한 것들을 찾을 수도 있습니다. 밥은 심지어 일부 벤더의 지원 라인에 전화를 걸어서 PotatoCom에서 걸려온 것으로 가장하고 PotatoCom이 고객인지 확인할 수 있습니다.

공격 분석

시스템 진입

시스템에 진입하는 가장 간단한 방법은 소셜 엔지니어링을 통해 누군가가 로그인을 위한 유효한 자격 증명을 제공하도록 만드는 것입니다. 밥은 관리자 자격 증명이 필요 없습니다. 인프라를 볼 수 있는 사람이면 수정을 할 수 없더라도 괜찮습니다. 거기서부터 네트워크 스캔을 사용하여 인프라를 탐색하고 소프트 타깃을 공격하기 위해 내부망 확산을 사용할 수 있습니다. 일단 시스템에 여러 개의 백도어가 있으면 밥은 데이터베이스 및 손상된 항목으로 들어가기 위해 기술적 요소를 사용할 수 있지만, 이는 어려운 방식입니다.

PotatoCom의 보안을 파괴하기 위해 밥에게 정말 필요한 것은 관리자 비밀번호입니다.

이 회사는 단일 클라우드 프로바이더에 전체 인프라를 두고 있으므로, 백업을 수행할 때처럼 생산 환경에 동일한 관리자 자격 증명을 사용할 가능성이 큽니다(보안에 정통한 관행은 아니지만, 이런 경우가 발생합니다).

대상 파악하기

밥은 소셜 엔지니어링으로 관리자 자격 증명을 보유한 사람에게 도달할 수 없을 가능성이 큽니다. 이들은 보안에 대한 경각심이 더 많기 때문입니다. 따라서 그는 적절한 대상을 파악하고 물리적 감시를 사용합니다.

밥은 대상에 대해 학습하며 그 지식을 사용해서 원하는 관리자 자격 증명을 얻을 한 가지 이상의 취약점을 찾을 것입니다.

예를 들어, 사무실은 물론이고 집도 절대 안전하지 않으며 자기 집에 있는 사람들을 감시할 기회는 많습니다. 대상이 재택근무를 하지 않는다면, 그들의 사무실은 어디입니까? 밥은 소셜 엔지니어링을 통해 오피스를 알아내고, 카메라 또는 키로거를 심거나 창문을 통해 염탐하거나 무선 키보드에서 신호를 가로챌 수 있습니다.

해커처럼 생각하기

PotatoCom의 인프라에 일단 연결하면 밥은 변경 사항 보고 기능을 비활성화하고 데이터베이스를 손상시킵니다. 그런 다음 이를 백업하고 오래된 백업을 지우며, PotatoCom의 암호를 변경하고 모든 증거를 파괴합니다.

PotatoCom의 금융 데이터베이스는 이제 사용할 수 없고, 오류를 알아내기 위해 계정에 액세스할 수 없습니다. 고객 청구, 공급업체 결제, 또는 세금 신고를 할 수 없습니다. 감사가 발동되고, 필수 데이터에 액세스하지 못해 어려움을 겪을 수 있습니다. 심지어 사업이 망할 수도 있습니다.

밥은 기술적으로 어려운 일을 하지 않았습니다. 중요한 것은 사고방식이었습니다. 밥은 들키지 않기 위해 무척 노력했습니다. 그리고 가장 쉬운 방법을 찾았습니다. 모든 시스템에서 공격하기 가장 쉬운 부분은 일반적으로 책임자이며, 이것이 해커가 생각하는 방식입니다.

해커를 물리치기 위해서 방어자는 안전 우선이라는 올바른 사고방식만이 필요합니다.

방어자는 해커처럼 생각해야 해서 공격당할 수 있는 부분을 찾고, 기술, 비즈니스 프로세스 또는 심지어 창문의 커튼을 사용해서라도 이 간극을 메워야 합니다. 방어자는 무엇을 방어할지 알게 되면 필요한 도구를 찾습니다. 해커와 마찬가지로, 방어자에게도 사고방식이 중요합니다.

고급 개념

규정 준수

인포섹 기술을 단순히 구현하거나, IT 정책을 체크 상자 방식으로 적용하여 심사를 통과하는 것은 점점 더 충분치 않아집니다. 조직은 기본 내용과 인포섹이 필요한 이유를 실제로 이해하고 있어야만 합니다.

예를 들어, 유럽 연합(EU)의 일반데이터보호규정(General Data Protection Regulation: GDPR)에서는 대규모 데이터 처리에 관여하는 조직에 데이터보호책임자(Data Protection Officer: DPO)를 보유하도록 규정합니다. DPO는 GDPR 준수를 보장해야 할 책임을 지며, DPO 또는 그들이 근무하는 조직이 EU 시민의 정보 보안에 태만하면 개인적으로 중요한 재정적 결과가 발생합니다.

세그멘테이션 및 마이크로세그멘테이션

네트워크 관리자는 세그멘테이션 및 마이크로세그멘테이션을 사용하여 네트워크 방어선의 방어를 통과하는 데 성공한 공격자의 내부망 확산을 방지합니다. 각 세그먼트(또는 한 개의 애플리케이션만 포함하는 마이크로 세그먼트)는 개별적으로 방어됩니다. 이러한 종류의 링 펜싱은 내부망 확산으로부터 보호하며, IT 인프라에 클라우드 서비스 프로바이더와 같은 멀티 테넌트가 있는 공유 환경에서 특히 중요합니다.

예를 들면 마이크로세그멘테이션은 연구 병원에서 유리할 것입니다. 각 연구 프로젝트가 자체 IT 인프라를 구매하는 대신, 마이크로세그멘테이션과 결합한 프라이빗 클라우드 및 적절한 인포섹 조치를 사용하여 각 프로젝트를 공유 병원 IT 인프라에서 테넌트로 분리할 수 있습니다.

종합적인 보안 솔루션

인포섹 보안 침해 이벤트는 삶의 일부입니다. 보안 침해가 필연적으로 일어난다고 해서 방지 기술이 무용지물인 것은 아니며, 조직은 보안 사고가 발생할 때 일어날 일에 대비해야 한다는 의미입니다.

탐지 및 완화 기술에 연동하면 자동화를 사용하여 네트워크 스위치에 보안 사고가 발생한 디바이스를 분리 또는 격리하도록 명령하는 등의 완화 단계를 트리거할 수 있습니다. 이는 내부망 확산을 방지하며, 기업은 이벤트당 수천만에서 심지어 수억 달러까지 절약할 수 있습니다.

예방, 탐지, 완화 및 사고 대응은 조직이 반드시 주의해야 할 인포섹 책임의 네 가지 영역이며, 가장 근본적인 수준에서 기본 IT 인포섹 방어는 사고방식이 중요하다는 점을 기억해야 합니다.

주니퍼 Connected Security

보안에는 계층이 필요합니다

최신 네트워크의 방어는 해당 네트워크상의 모든 것을 방어한다는 의미이며, 대부분의 조직이 실행하는 것과는 다른 인포섹 접근 방식이 필요합니다.

네트워킹 및 보안은 상호 연결되어 있으며, 사람들이 포인트 솔루션을 사용하여 네트워크를 설계하려 할 때 심각한 문제가 발생하는 경향이 있습니다. 효과적인 네트워크 보안은 여러 벤더의 여러 기술을 구축하여 달성한 다계층을 상호연결할 때 가능합니다.

주니퍼 Connected Security에 포함되는 스위치, 라우터 및 Wi-Fi 액세스 포인트는 모두 중앙 자동화 및 오케스트레이션을 통해 심층 네트워크 가시성 및 네트워크 정책 적용 지점을 제공합니다. 이로써 달성하기 어려울 수 있는 내부 확산 방지(lateral protection)를 조직에 제공합니다.

분석가들은 한 특정 세그먼트에 대한 최상의 솔루션은 하나의 전문 포인트 업체가 제공할 가능성이 높다고 말하지만, 이러한 접근 방식은 조직이 여러 제품을 사용하고, 다양한 부분이 모두 서로 잘 작동해야만 가능합니다. 이렇게 되면 네트워크 방어의 자동화 및 오케스트레이션이 어려워질 수 있습니다. 순위는 항상 변하고, 자동화 구현은 자동화한 제품의 수명 주기를 넘어버리는 경우가 많습니다.

많은 벤더는 파트너 생태계를 비롯한 다양한 네트워킹 및 인포섹 제품 포트폴리오를 갖추고 있습니다. 주니퍼와 같은 여러 다른 벤더가 서비스 프로바이더 규모로 운영하는 고객을 지원하며, 엔터프라이즈 고객이 상상할 수 있는 최고 규모의 엄청난 네트워크를 처리할 수 있습니다.

주니퍼의 차별화 요소는 상호연결에 대한 약속인 주니퍼 **Connected Security**에 '연결'되어있다는 점입니다. 주니퍼는 통합 및 오케스트레이션에 뛰어나며, 개방형 표준, 개방형 프로토콜 및 개방형 API의 사용을 장려하고 심지어 경쟁 제품을 지원하는 구축도 합니다. 우리의 목표는 고객이 기존의 것을 제거하고 교체하도록 요구하기보다는 이미 가지고 있는 것을 최대한 활용하게 돕는 것입니다.

주니퍼의 포트폴리오 전반에서 단일 운영체제인 Junos를 사용하면 중앙 집중식 관리를 훨씬 단순화할 수 있고, 주니퍼는 온프레미스, 클라우드 기반 또는 둘을 조합한 관리 플랜으로 풍부한 기능의 관리 플랫폼을 제공할 수 있습니다. Junos OS에서는 경제적으로 포트폴리오 전반에 걸쳐 기능을 추가할 수 있습니다.

주니퍼 Connected Security는 네트워크 전반의 모든 연결 지점으로 보안을 확대하여 사용자, 애플리케이션, 인프라를 보호할 수 있는 기능을 조직에 제공합니다. 가능한 한 위협에 가깝게 정책을 적용하면 위협 확산의 위험을 줄일 수 있습니다. 그리고 머신러닝, 고급 분석 및 자동화를 통해 신속한 사고 대응을 실현합니다.

주니퍼 Connected Security의 실제 적용 사례를 알아보세요.

자세히 보기

사이버보안 베이직 교재 전체를 확인하려면 여기를 클릭하세요.

JUNIPER NETWORKS | Engineering Simplicity

PN: 7400127-001-KR

기업 및 세일즈 본부
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
전화: 888.JUNIPER (888.586.4737)
또는 +1.408.745.2000
팩스: +1.408.745.2100
www.juniper.net

APAC 및 EMEA 본부
Juniper Networks International B.V.
Boeing Avenue 240
우편번호 06236
Amsterdam, The Netherlands
전화: +31.0.207.125.700
팩스: +31.0.207.125.701