Microsoft Security

비즈니스 보호하기: 사이버 보안 101

사이버 보안 위협은 비즈니스를 중단시키고, 민감한 데이터를 훔치고, 몸값을 요구할 수 있습니다. 사이버 보안 환경과 비즈니스를 보호하는 방법에 대해 알아보세요.

사이버 보안 위협은 외부와 내부, 두 가지 형태로 나뉩니다.

외부 위협

외부 위협은 귀사의 네트워크를 표적으로 삼습니다. 공격자는 트래픽으로 압도하려고 시도하기 때문에 귀사에서 비즈니스를 운영하는 데 필요한 시스템에 액세스할 수 없게 합니다. 네트워크 공격에는 다음과 같이 크게 두 가지 유형이 있습니다.

DoS(서비스 거부)

컴퓨터가 대상 서비스를 압도하기 위해 네트워크 서비스에 많은 요청을 보내는 공격입니다.

DDoS(분산형 서비스 거부)

DoS 공격과 마찬가지로, 이는 협조 공격 (coordinated attack) 방식으로 여러 위치에서 다수의 컴퓨터를 사용하여 시도됩니다.

네트워크 보호하기

Azure DDoS Protection Standard는 DDoS 공격을 방어하는 데 도움이 됩니다. 가상 네트워크의 모든 퍼블릭 IP 주소를 보호하도록 자동으로 조정됩니다.

내부 위협

내부 위협은 사람들을 표적으로 삼습니다. 공격자들은 소셜 엔지니어링 전술을 사용하여 사용자가 개인 인증 정보를 제공하거나 중요한 정보를 공개하도록 속입니다.

일반적인 공격은 다음과 같습니다.

피싱 및 스피어 피싱

사기꾼들은 동료, 친구 또는 평판이 좋은 사람이나 회사로부터 링크나 첨부 파일이 포함된 이메일을 직원들에게 보냅니다. 직원이 링크를 클릭하거나 첨부 파일을 열면 공격자가 시스템에 액세스할 수 있습니다.

비싱 (Vishing)

이는 피싱과 비슷하지만 이메일 대신 전화 통화를 활용합니다.

베이팅 (Baiting)

공격자가 피싱 또는 비싱 공격에 대응하기 위해 가짜 상품을 제공하는 경우를 말합니다.

브라우저 공격

이러한 공격은 브라우저 확장 프로그램을 설치하기 위한 팝업 광고 또는 제안으로 나타날 수 있습니다.

네트워크 보호하기

1. 직원들에게 안전한 이메일 및 브라우징 사용에 대한 교육을 제공하세요. 자세히 알아보세요.
2. 직원들이 온라인 상태일 때 발생할 수 있는 위험을 이해하도록 지원하세요. Microsoft의 기타 Microsoft가 제공하는 기타 사이버 보안 교육 인포그래픽(개인 데이터와 디바이스를 안전하게 보호하기 위한 10가지 쉬운 규칙, 피싱으로부터 자신을 보호하는 7가지 방법, 기술 지원 스캠으로부터 자신을 보호하기 위한 5가지 프로 팁)을 동료들과 공유하세요.
3. Microsoft Defender for Office 365을 활용하여 공격 시뮬레이션 교육을 제공하세요.
4. 암호를 사용하지 않고 다중 인증을 사용하세요.
5. 모든 회사 디바이스가 최신 버전의 Windows 및 인터넷 브라우저를 사용하는지 확인하세요.
6. 회사 파일 저장 프로토콜을 적용하세요. 회사 데이터를 클라우드에 안전하게 저장하고 암호화하세요.
7. 직원들에게 HTTPS와 같은 보안 연결 사용의 중요성을 교육하세요. 브라우저에 HTTPS Everywhere 플러그인을 설치하세요.
8. 직원들과 함께 웹 사이트의 ID를 확인하기 위해 웹 사이트 인증서를 확인하는 관행을 만드세요.
9. 기본적으로 팝업 차단을 사용하도록 설정하세요.
10. Microsoft Windows Defender와 같은 클라우드 기반 바이러스 백신 솔루션을 사용하세요.

Microsoft Security의 인사이트에 대한 보다 자세한 내용은 www.microsoft.com/security/business/cybersecurity-awareness에서 확인하세요.

더 많은 사이버 보안 모범 사례 공유하기

Microsoft