OUCH! | 2018 년 12 월 호

SANS SECURITY AWARENESS

OUCH!

전 국민대상 월간 정보보호 인식제고 뉴스레터

우리가 바로 공격대상입니다

개요

많은 사람들이 자신이 사이버 공격의 대상이 아니라고 잘못 믿고 있습니다. 자신들의 시스템이나 계정은 공격받을 만큼 가치가 없다는 것입니다. 이것은 더 이상 진실이 아닙니다. 어쨌든 직장이나 가정에서 기술을 사용한다면, 우리 자신은 나쁜 사람에게 큰 가치가 있습니다. 그러나 운 좋게도 이 글을 읽고 있다면 이미 사이버 공격에 대응할 수 있는 최고의 방어력을 가지고 있습니다.

왜 우리가 공격대상인가

오늘날 인터넷에는 다양한 사이버 공격자가 존재하며 서로 다른 동기를 가지고 있습니다. 그러면 왜 이들은 우리를 공격하고 싶어할까요? 해킹을 하면 자신들의 목표를 달성하는 데 도움이 됩니다. 다음은 사이버 공격자의 두 가지 일반적인 예와 이들이 우리를 공격대상으로 삼는 이유입니다.

⚠ **사이버범죄자**: 이 사람들은 가능한 한 돈을 많이 버는 것이 목적입니다. 인터넷이 이 사람들에 중요한 이유는 버튼을 누르기 만하면 전 세계 모든 사람을 쉽게 공격할 수 있다는 것입니다. 그리고 이들이 온라인을 통해 돈을 벌 수 있는 방법이 많이 있습니다. 예를 들어, 은행이나 연금 계좌에서 돈을 훔치거나, 우리 이름으로 신용 카드를 만들고, 청구서를 보내거나, 컴퓨터를 사용하여 다른 사람을 해킹하거나, 소셜 미디어 또는 게임 계정을 해킹하여 다른 범죄자에게 판매하는 행위 등이 있습니다. 나쁜 사람이 인터넷을 이용해서 돈을 벌 수 있는 방법을 거의 무한합니다. 매일 수십만 명의 나쁜 사람들이 우리 자신을 포함해서 가능한 한 많은 사람들을 해킹한다는 목표로 매일 아침 일어나서 일하고 있습니다.

☆ **표적공격자**: 이들은 고도로 숙련된 사이버 공격자이며, 정부, 범죄단체 또는 경쟁기업을 위해 일하면서 우리가 속한 회사를 노리고 있습니다. 여러분들은 본인의 일이 큰 관심을 끌지 않을 것이라고 생각하지만, 사실은 다릅니다. 패스워드가 맞는데도 패스워드가 맞지 않다고 나옵니다.

- 직장에서 다루는 정보는 다른 회사나 정부에 엄청난 가치가 있습니다.

- 표적형 공격자는 회사에서 일하는 우리를 공격할 수 있습니다. 우리를 해킹하기 위해서가 아니라 다른 동료나 다른 시스템 중 하나를 해킹하기 위해서입니다.
- 이러한 종류의 공격은 우리를 먼저 공격하여 우리와 같이 일하는 기업이나 파트너사를 공격하기 위해서입니다.

안티바이러스만 있으면 안전한가?

"좋아. 나는 공격대상이지만 문제는 없어. 내 컴퓨터에 바이러스 백신과 방화벽을 설치하면 보호받을 수 있어. 그렇죠?" 하지만 안타깝게도 아닙니다. 많은 사람들은 보안 도구를 설치하면 안전하다고 생각합니다. 불행히도, 이 말은 완전히 사실이 아닙니다. 사이버 공격자는 계속 발전하고 있으며, 공격 방법 대부분은 지금의 보안 기술을 쉽게 우회합니다. 예를 들어 바이러스 백신이 탐지할 수 없는 특별한 악성코드를 만드는 경우가 있습니다. 사용자 정의 피싱 공격으로 이메일 필터를 우회하거나, 보이스피싱 전화를 걸어 신용카드 번호, 개인정보, 돈 또는 비밀번호를 빼냅니다. 기술은 당신을 보호하는 데 중요한 역할을 하지만, 궁극적으로 본인이 최선의 방어선입니다.

다행히도 보안은 그다지 어렵지 않으며, 궁극적으로는 상식적으로 접근해야 하며 일부 기본적인 접근하는 것이 최선의 방어입니다. 매우 긴급하거나 이상하거나 의심스러운 이메일, 메시지(카톡) 또는 전화를 받는 경우 공격일 수 있습니다. 컴퓨터와 기기의 보안을 유지하려면 자동 업데이트를 사용하십시오. 마지막으로 온라인의 각 계정마다 강력하고 고유한 패스워드를 사용하십시오. 사이버보안을 인식하는 것이 궁극적으로 최선의 방어입니다. 무엇을 시작할 지 모르십니까? 그렇다면 월간 SANS OUCH! 뉴스레터를 구독하십시오!.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

객원 편집자

맷 브로밀리 (@mbromileyDFIR)는 사고대응가이자 디지털 포렌식 전문가로서 8년 이상의 경험을 가지고 있으며 전 세계의 조직 및 사고를 대응하고 있다. 매튜는 또한 디지털 포렌식 및 사고대응 강사이며 SANS FOR508 및 FOR572 과정을 가르친다.

SANS SECURITY AWARENESS

참고자료

악성코드 차단: https://www.sans.org/u/L1J
사회공학: https://www.sans.org/u/L1O
보이스피싱 전화사기: https://www.sans.org/u/L1T
패스워드: https://www.sans.org/u/L1Y
포스터 - You Are a Target: https://www.sans.org/u/L23