OUCH! | 2016 년 11 월호

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 클라우드 회사 선택
- 데이터 보호 방법

클라우드 서비스 안전한 사용방법

개요

"클라우드"는 사람들마다 서로 다른 의미로 사용되지만 일반적으로 클라우드 서비스 회사를 이용해서 인터넷에 데이터를 저장하고 관리하는 것을 의미합니다. 클라우드의 장점은 전 세계에서 어디든 다양한 기기에 있는 데이터에 접근하고 동기화할 수 있을 뿐만 아니라, 다른 사람들과 정보를 공유할 수 있습니다. 이러한 서비스를 "클라우드"라고 부르는 이유는 데이터가 물리적으로 저장되어 있는 위치를 모르기 때문입니다. 클라우드 컴퓨팅 서비스 예로는 구글 닥스(Docs)에서 문서를 생성하고, 드롭박스를 통해 데이터를 공유하고, 아마존 클라우드에서 서버를 구축하고, 세일즈포스에서 고객 데이터를 저장하거나 애플 아이클라우드에 음악이나 그림을 저장하는 것 등이 있습니다. 이러한 온라인 서비스를 이용하면 좀 더 생산적일 수 있으나, 고유한 위험이 있습니다. 이번 호에서는 클라우드를 안전하게 사용할 수 있는 방법에 대해서는 다룹니다.

객원 편집자

데이브 쇄클포드(트위터 @daveshackleford)는 부두 보안을 소유한 전문 컨설턴트이며, SANS 교육과정 SEC579(가상화 및 프라이빗 클라우드 보안) 및 SEC524(클라우드 보안) 등의 저자이다.

클라우드 회사 선택

클라우드는 좋은 것도 아니고 나쁜 것도 아닙니다. 클라우드 서비스는 직장과 집에서 일하기 위한 도구일 뿐입니다. 하지만 클라우드를 이용할 때 개인적인 정보를 모르는 사람들에게 넘겨주고, 서비스 회사에서 보안성과 가용성을 지켜주기를 기대합니다. 그래서 현명하게 클라우드 서비스 회사를 선택해야 합니다. 사무실 컴퓨터 또는 업무와 관련된 정보의 경우에는, 먼저 상사에게 클라우드 서비스를 사용할 수 있는 지 문의해야 합니다. 클라우드 사용이 가능하면 어떤 클라우드 서비스를 사용할 수 있는 지, 정책 및 사용방법도 확인해야 합니다. 클라우드를 개인적으로 사용하고자 한다면, 다음 사항을 고려해보기 바랍니다.

1. **지원**: 클라우드 회사로부터 쉽게 도움을 받을 수 있는 지, 질문에 대한 답을 받을 수 있는가? 연락할 수 있는 전화나 이메일이 있는가? 회사 웹사이트에 공개된 포럼이나 FAQ를 가지고 있는가?
2. **단순함**: 서비스를 쉽게 이용할 수 있는가? 서비스가 복잡할수록 실수하거나 실수로 정보를 외부로 노출 시킬 수 있습니다. 쉽게 이해하고, 구성 및 사용할 수 있는 클라우드 서비스를 사용하는 것이 좋습니다.

클라우드 서비스 안전한 사용방법

3. **보안**: 어떤 데이터가 수집되는가? 그렇다면 여러분의 컴퓨터나 기기에서 어떤 방법으로 클라우드로 데이터가 전송되는지, 클라우드에 어떻게 저장되는지, 데이터가 암호화되는 지 그렇다면 , 누가 데이터를 해독할 수 있는가?
4. **약관**: 시간을 내서 약관을 검토해보는 것이 좋습니다. 누가 우리 데이터에 접근할 수 있는 지, 우리가 가질 수 있는 법적인 권한이 무엇인지, 서비스 업체 및 이용자의 보안 책임은 무엇인지 확인해야 한다.

클라우드를 이용하면 데이터에 쉽게 접근할 수 있고 생산적이지만, 정보를 저장 및 공유하는 방법에 대해서 주의해야 합니다.

데이터 보호 방법

클라우드 서비스를 선택하였다면, 그 다음은 그 회사의 서비스를 제대로 사용할 수 있는지 확인하는 것입니다. 데이터 접근 및 공유 방법은 다른 어떤 것 보다 데이터 보안에 중요한 요소이다. 다음은 정보를 보호할 수 있는 몇 가지 중요한 조치 단계입니다.

1. **인증**: 클라우드 계정을 인증하기 위해서는 강력하고 긴 패스워드를 사용해야 합니다. 클라우드 공급회사에서 2 단계 인증을 제공한다면, 이 방법을 사용하기 바란다. 이 단계는 계정을 지킬 수 있는 가장 중요한 단계 중 하나입니다.
2. **파일 및 폴더 공유**: 클라우드는 아주 쉽게 데이터를 공유할 수 있습니다. 우리는 특정한 사람에게만 파일을 공유 공유한다고 생각할 수 있지만, 최악의 경우 뜻하지 않게 파일 또는 전체 폴더를 인터넷에 공유할 수 있습니다. 우리를 보호할 수 있는 가장 좋은 방법은 아무하고나 파일을 공유하지 않는 것이다. 그 다음엔 오직 반드시 알아야 만 하는 사람에게만 특정 파일이나 폴더에 특정인(또는 그룹 사람들)만 접근할 수 있도록 해야 합니다. 더 이상 파일에 접근할 필요가 없는 사람이 있다면 제거해야 한다. 클라우드 회사에서는 파일 및 폴더에 누가 접근하였는지 추적하는 방법을 제공하고 있습니다.
3. **링크를 통한 파일/폴더 공유**: 일부 클라우드 서비스의 일반적인 기능에는 파일 또는 폴더로 연결되는 웹 링크를 생성해 줍니다. 이 기능을 이용하면 웹 링크를 제공해서 원하는 사람과 파일을 공유할 수 있습니다. 하지만 이 기능은 보안성이 낮으며, 이 링크를 알고 있는 사람은 누구나 개인적인 파일 또는 폴더에 접근할 수 있습니다. 만약에 한 사람에게 링크를 보내면, 그 사람이 다른 사람과 이 링크를 공유할 수 있으며, 검색엔진에서 검색결과로 나올 수 있습니다. 만약에 링크를 이용해서 데이터를 공유한다면, 사용기간이 끝나면 링크를 삭제하거나, 패스워드로 링크를 보호해야 합니다.

클라우드 서비스 안전한 사용방법

4. **설정**: 클라우드 회사에서 제공되는 보안 설정 방법을 이해해야 합니다. 만약에 여러분이 다른 사람과 폴더를 공유하고 있다면, 그 사람이 우리가 모르게 다른 사람에게 우리 데이터를 공유할 수 있는가? 또한 공유한 파일을 누가, 언제 보았는 지 확인할 수 있는 수단이 있는 지도 확인해 보시기 바랍니다. 공유할 때 "읽기만" 가능한지 누구나 수정할 수 있는 "읽기+쓰기"가 가능하도록 제한이 가능한지도 확인이 필요합니다.
5. **안티바이러스**: 사용하고 있는 컴퓨터와 데이터공유에 사용되는 모든 컴퓨터에 최신 버전의 안티바이러스 소프트웨어가 설치되어야 합니다. 공유 파일이 감염되면 동일한 파일에 접근하는 다른 컴퓨터도 마찬가지로 감염될 수 있습니다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

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.

참고자료

2단계 인증:	https://securingthehuman.sans.org/ouch/2015#september2015
패스워드:	https://securingthehuman.sans.org/ouch/2015#april2015
패스워드 관리프로그램:	https://securingthehuman.sans.org/ouch/2015#october2015
악성코드란 무엇인가?:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley, 번역:진수희(ITL Inc.)