스타트업의 생존 보안

2023.06

(주)스푼라디오 정보보안팀 김태열
개인정보보호위원회 개인정보전문 강사

- 이름 : **김태열.** CPPG, CISA, ITIL, PMP, ISO27001심사원(보), 사회복지사
- 소속 : **(주)스푼라디오 (https://www.spooncast.net/kr)**
- 주요경력 :

  현) 개인정보보호위원회 개인정보보전문강사

  전) (주)위메이드플레이 (구 – 선데이토즈) 개인정보보호 팀장

  전) 월드비전 개인정보 및 정보보호 총괄

  전) SK커뮤니케이션즈 고객인프라팀 팀장

목소리로
서로의 팬이 되는 곳

2016년, 스푼은 보통의 소소한 이야기를 전화 통화하듯
목소리로 편하게 나눌 수 있게 해보자라는 아이디어로 시작되었습니다.
스푼은 이제 누구나 쉽고 편하게 오디오 방송을 할 수 있는 플랫폼에서
목소리로 소통하고 서로가 서로의 팬이 될 수 있는
오디오 소셜 플랫폼으로 거듭나고 있습니다.

스푼라디오 소개 - 2

Spoon

Mission

사람들의
이야기로
세상을
연결한다

Vision

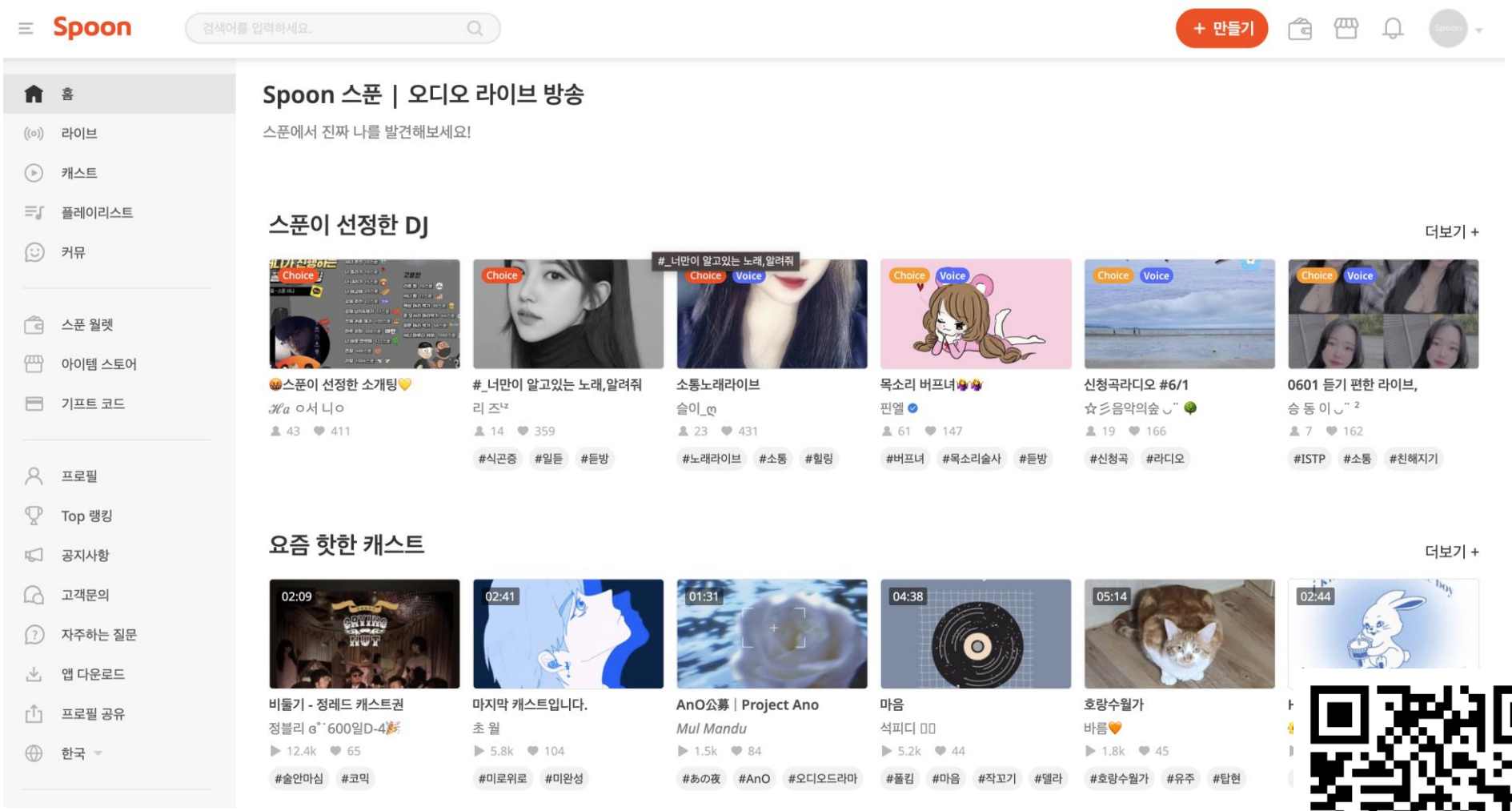
누구나 쉽고 빠르게 이야기할 수 있게 한다

스푼은 다양한 사람들의 이야기를 담고, 연결시켜주는 새로운 힘이 되고자 합니다.
누구나 언제든 자신의 모습을, 목소리로 쉽고 편하게 표현할 수 있고
세상의 다양한 사람들과 이야기를 나누며 진정성 있는 관계를 맺을 수 있도록

https://spoon.onelink.me/v75r/pj1ury82

스푼라디오 소개 - 3

Spoon

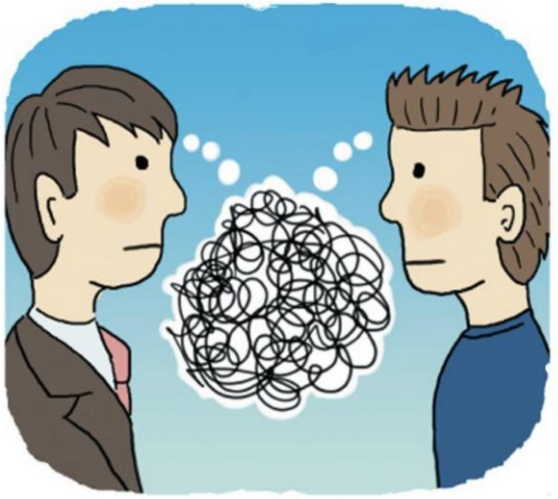


https://spoon.onelink.me/v75r/pj1u

발표하기 전에...

Spoon

1. 제가 속한 회사가 다른 회사보다 보안을 잘한다고 생각하지 않습니다.
   (잘해 놓은 부분은 모두 전임자 분이 해주셨어요)
2. 여기에 혹시나 사례 또는 기사의 캡쳐는 제가 최신기사 기준으로 무작위로 작성한 겁니다.
3. 해당 내용은 온전히 개인적인 경험에서 나온 부분입니다. 주관적일 수 도 있지만 발표자의 경험에 의한 것이니 오해 하지 말아 주세요 ~~~



이미지 출처 : https://www.donga.com/news/Opinion/article/all/20210705/107804113/1

스타트업의 개인정보 유출 사고

Spoon


ChosunBiz

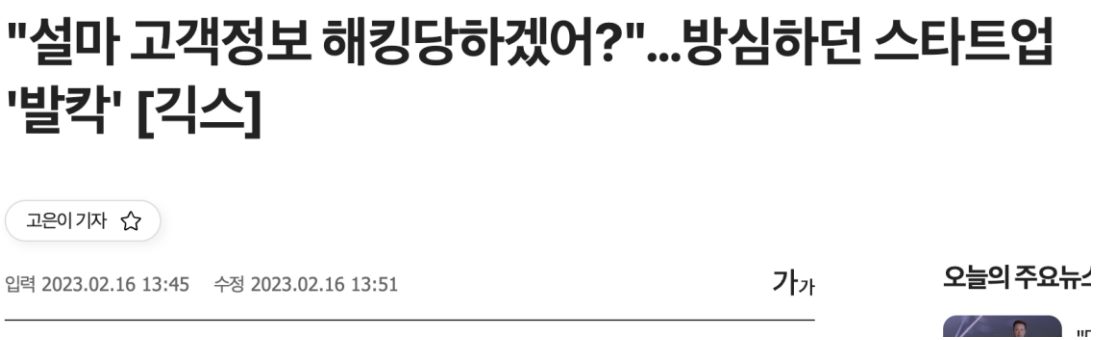
출처 : 조선비즈 입력 2022.06.08 06:00

증권 부동산 IT 금융 산업 Car 유통 정책 정치 사회 국제 사이언스조선 오피니언 이코노미조선

IT > ICT

밀 재· 빌 도 해킹당했다… 보안 취약한 스타트업 노리는 '검은 손'

해킹으로 고객 개인정보 유출 사고 발생
스타트업, 해킹 피해로 상장·투자도 휘청
자본·인력 투입해 보안솔루션 갖춰야 지적


"설마 고객정보 해킹당하겠어?"...방심하던 스타트업 '발칵' [긱스]

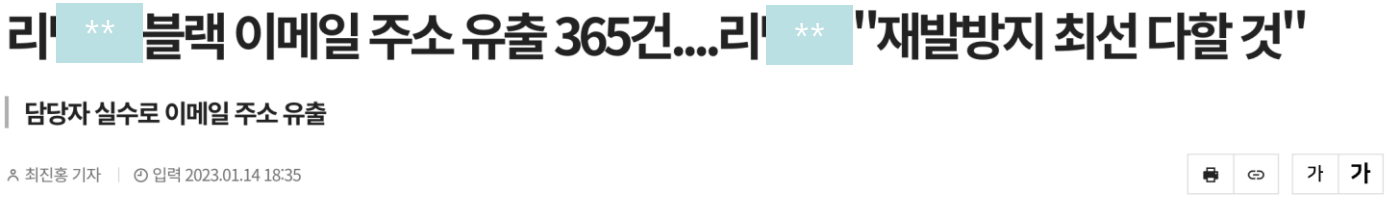
고은이 기자

입력 2023.02.16 13:45 수정 2023.02.16 13:51

가가

오늘의 주요뉴스

출처 : 한경
https://www.hankyung.com/it/article/2023012782227i


리** 블랙 이메일 주소 유출 365건....리** "재발방지 최선 다할 것"

담당자 실수로 이메일 주소 유출

최진홍 기자 | 입력 2023.01.14 18:35

가 가

출처 : https://www.econovill.com/news/articleView.html?idxno=600336

그래서 고민을 해봤습니다.

Spoon

스타트업 보안담당자들의 고민은 뭘까?

어떤 부분이 잘하고 있지?

전임자가 잘해 놓았는데
내가 더 잘할 수 있는 부분은 뭘까?

우리회사는 잘하고 있나?

사진출처 : https://blog.speak.com/kr/in-english/expressions/%EC%A0%90%EC%8B%AC-%EB%A9%94%EB%89%B4-%EA%B3%A0%EB%AF%BC%EC%9D%B8-%EC%82%AC%EB%9E%8C-%EA%B3%A0%EB%AF%BC%ED%95%98%EB%8B%A4-%EC%98%81%EC%96%B4%EB%A1%9C-%ED%91%9C%ED%98%84%ED%95%98%EA%B8%B0

최고경영자의 의지!!

Spoon 스푼라디오의 **핵심가치**

저 지금 잘하고 있나요? Am I doing well?

피드백 주셔서 고맙습니다! Thank you for your feedback!

말하지 않으면 모른다 Share to be aware

건강하게 충돌하되 결정되면 '확실하게' 지지한다
Healthy Conflict Leads to Full Commitment

틀에서 벗어난 생각 Think outside the box

절대 절대 절대 포기하지 않는다 NEVER NEVER NEVER give up

셀프스타터: 스스로를 동기부여하고 절제하며 돌아보기
Be a self-starter: self-motivated, self-disciplined, self-reflective

사용자가 아닌 팬을 만든다 Have fans not users

- 매주 Security Meeting 진행

  → *저 지금 잘하고 있나요?, 피드백 주셔서 고맙습니다.*

- ISMS-P 범위에 대한 결정 후 적극적인 지지

  → *건강하게 충돌하된 결정되면"확실하게 " 지지한다.*

- 지속적인 1 on 1 미팅 등

  → *말하지 않으면 모른다.*

ISMS-P, CBPR

스푼라디오 국내 온라인 서비스 운영(임직원 개인정보 처리 포함)
2020년 11월 18일 ~ 2023년 11월 17일

+

출처 : 개인정보보호 국제협력센터https://www.privacy.go.kr/pic/cbpr_info.do

왜? ISMS-P, CBPR 인가?

Spoon

Why? ISMS-P

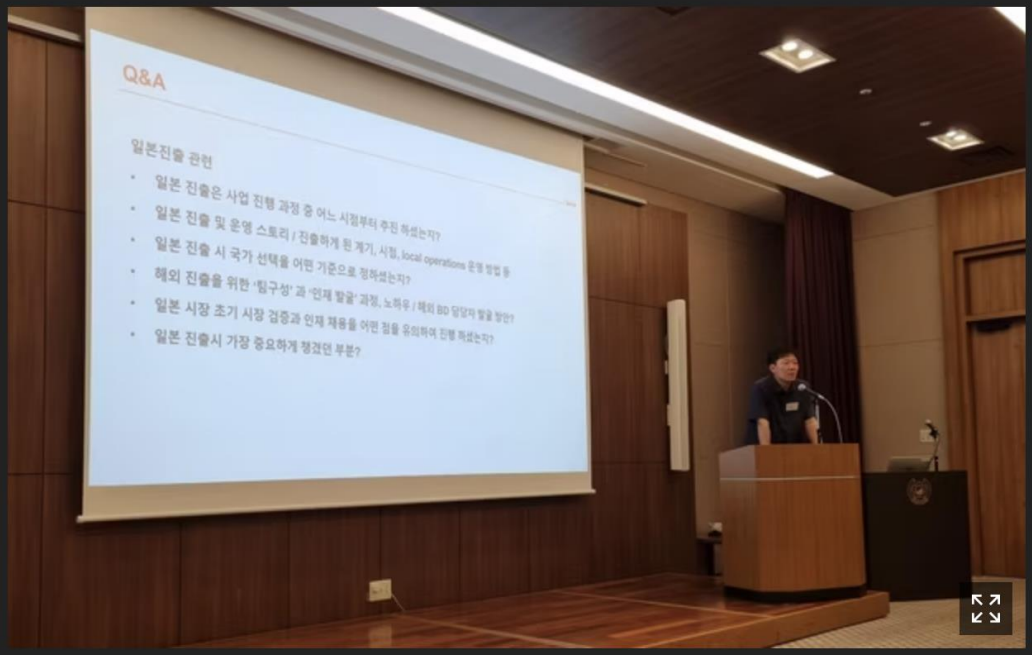
- 스푼라디오는 ISMS 인증 의무 대상 입니다.
- 하지만 스푼라디오는 ISMS-P 범위로 하여 인증을 받았습니다.
- ISMS-P를 통해 스푼라디오 서비스에 대한 전체적인 개인정보흐름을 한눈에 볼 수 있고
- 신규서비스 오픈시 개인정보흐름표 및 흐름도를 업데이트하여 발생할 수 있는 ISSUE를 한눈에 볼 수 있습니다.
- 범위를 임직원 개인정보 처리까지 포함하여 내•외부 개인정보 이슈를 식별하여 해결하기 위한 고민을 함께 할 수 있었고...
- 무엇보다 임직원분들의 보안에 대한 의식 수준을 올릴 수 있었습니다.
  (ISMS는 우리 회사 모든 구성원이 관심 갖고 해야 하는 일로 인식)

왜? ISMS-P, CBPR 인가?

Spoon

Why? CBPR

스푼 일본서비스 모습. /스푼라디오



도쿄스타트업포럼에서 발표를 하는 최혁재 스푼라디오 대표. /임경업 기자

출처 : 도쿄에서 스푼에게 듣는 일본 진출기 https://www.chosun.com/economy/smb-venture/2023/04/14/XAQZMZBQ4BGPHNXPCQLLSV7BGQ/

Why? CBPR

- 모든 KPI의 60%가 일본에서 들어오고 있으며...

- 2021년부터 시행된 개정 개인정보보호법에서는 외국에 있는 제3자에게 개인데이터를 제공할 때에는 해당 외국에서의 개인정보보호에 관한 제도나 개인정보보호를 위한 안전조치 등에 대한 환경파악과 ***개인 데이터의 안전한 관리를 위해 필요한 적절한 조치를 취해야 함을 의무화***하면서 **개인데이터 해외 이전에 대한 기업의 책임이 강화** (법 제28조)
  - 단, 개인정보보호법 시행규칙 제16조의2에 따르면 개인 데이터를 제공받는 자가 개인정보 취급과 관련된 국제적인 틀에 근거한 인정을 받고 있는 경우 제28조의 해외 제3자 제공 제한에서 제외되며, 관련하여 ***CBPR을 취득하는 것을 가이드라인에서 제시***하고 있음

자료출처 : CBPR인증제도 설명회 글로벌 개인정보 이전 환경에서 CBPR 인증의 의의 고려대학교 정보보호대학원 김법연 (22.5.17)

참고자료 : https://www.jipdec.or.jp/project/cbpr.html

몸은 가볍게 시스템은 최소화

Spoon

- 접근권한
  - 최소한의 권한 부여 등 (조회, 입력, 변경, 삭제…등)
  - 개별계정 발급
  - 안전한 비밀번호 설정 및 작성 규칙
  - 추가적인 인증 적용 (OTP 등)
  - 장기 미접속 차단 등
  - 접근권한 변경 또는 말소 신청, 기록 등

- 접근통제

사진출처 및 재인용 : https://bigsong.tistory.com/20

- 프로세스 강화
- 슬랙의 채널(#)을 통한 결재 및 알람
- Open 소스 활용
- 보안솔루션 등 온프레미스(On-Premise)인프라 최소화

가능한 부분은 프로세스로~~~

Spoon

개인정보의 기술적 관리적 보호조치 제4조 접근통제 (6월8일 현재 기준)

⑥ ***전년도 말 기준 직전 3개월간 그 개인정보가 저장. 관리되고 있는 이용자 수가일일평균 100만명 이상***이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) ***매출액이 100억원 이상인 정보통신서비스 제공자***등은 개인정보처리시스템에서 개인정보를 ***다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한접근권한을 설정할 수 있는 개인정보취급자***의 **컴퓨터 등을 물리적 또는 논리적으로 망분리** 하여야 한다.

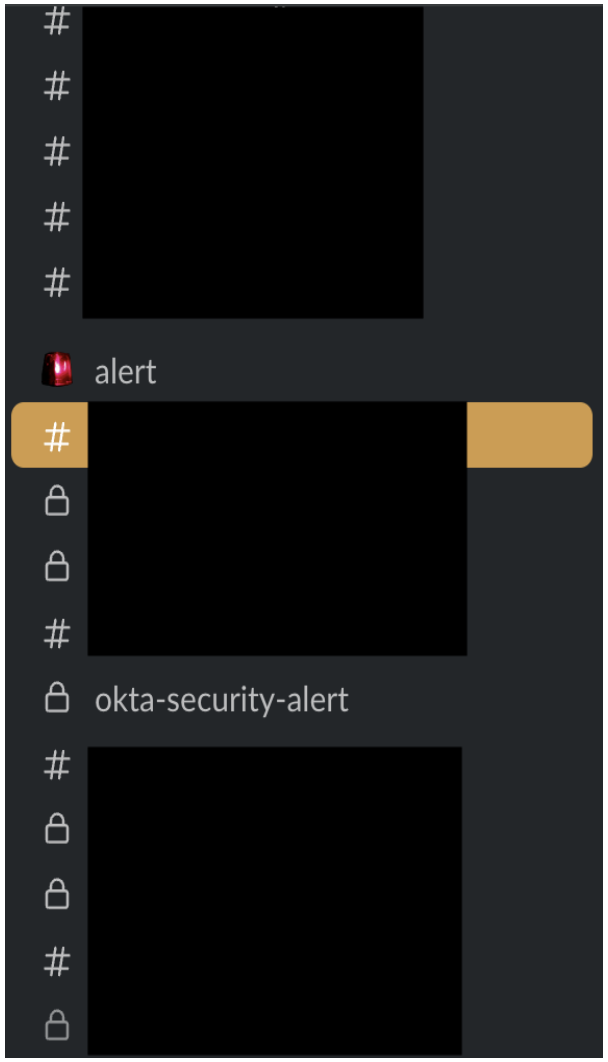
- **전제조건**
  - 논리적, 물리적 모두 비용이 만만치 않아요.
  - 법적요건을 최대한 만족해야 해요.
  - 현재 이용하고 있는 인프라에서 큰 변경사항이 없어야 해요

기존에 사용하던 인프라 (Cloud) + 정책 + 프로세스

협업을 위해 자사에서 이용하는 툴 최대한 활용

Spoon

*** Slack 봇을 활용한 Alert**



*** Confluence 를 활용한 정책 및 프로세스 가이드**

*** 구글 드라이브**

스타트업에서 보안은....

Spoon

사진출처 및 재인용 : https://blog.naver.com/haechiseoul/221629137932

Q & A