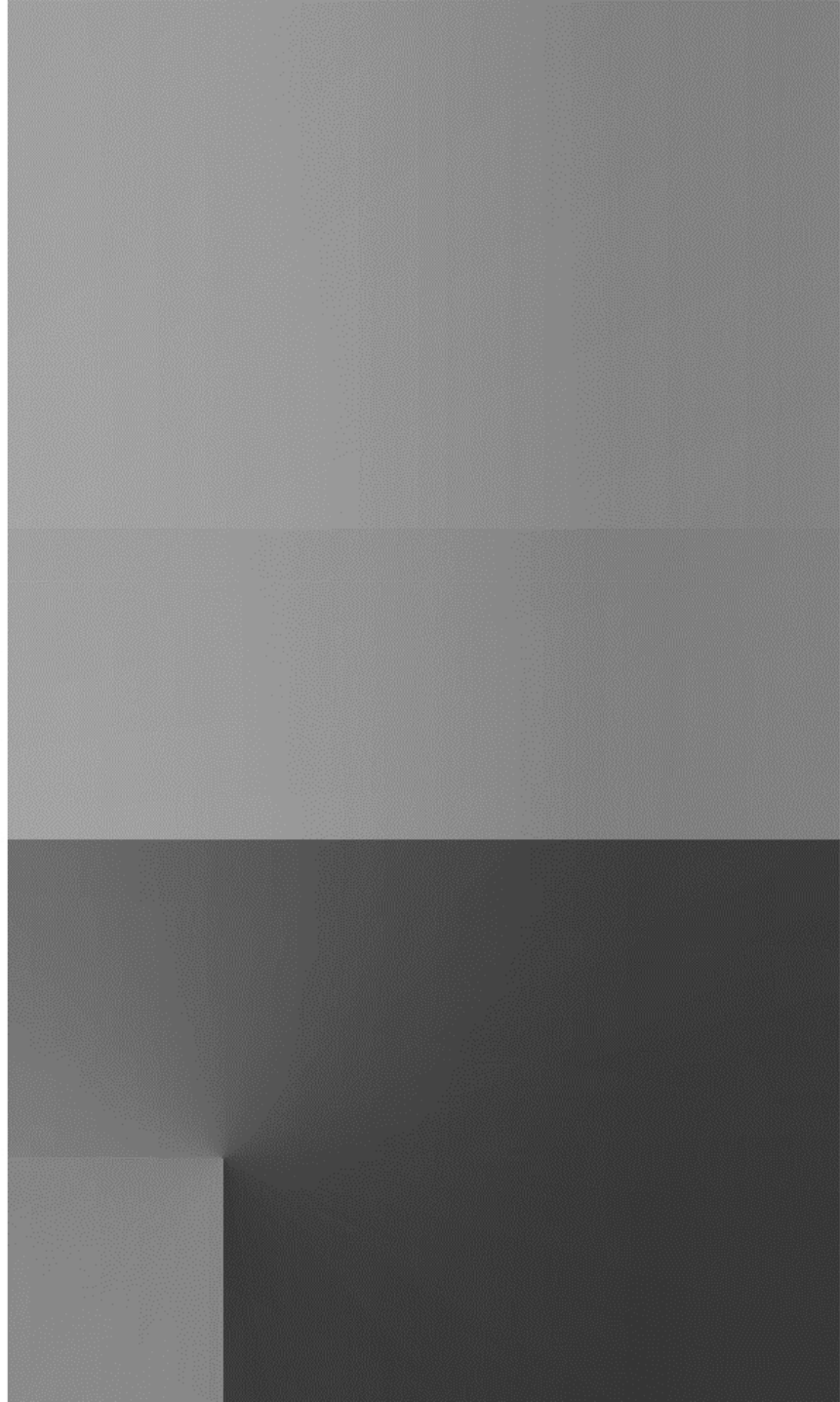
dongguk UNIVERSITY

정보보호 개론 “12주차 강의”

윤홍수

2025. 05. 22

Table of Contents



사이버 공격 대상

- **대한민국 IT 대기업이 사이버 공격에 취약한 이유**
  1. 높은 공격 가치
  2. 핵심 기술 및 기업 비밀
  3. 국가 배후 해킹 그룹
  4. 구조적인 보안 취약점
  5. ..

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

1. 높은 공격 가치
   - IT 대기업들은 소셜 미디어, 통신, 전자상거래, 금융 등 매우 광범위한 서비스를 제공
   - 수천만 명 이상의 개인 정보를 보유
   - 해커들에게는 엄청난 가치를 지니는 황금알
   - 개인 정보 유출은 2차 금융 사기, 스미싱, 피싱 등 다양한 범죄로 이어질 수 있어 공격자들에게 매력적인 목표

사이버 공격 대상

https://m.boannews.com/html/detail.html?idx=124626

국내 기업의 정보보호 투자 현황... 투자액 상위 10대 기업은 어디?

순위	23년					22년	
	기업명	업종	투자액	순위 변동	투자 비중	기업명	투자액
1	삼성전자	제조업	2,435	-	5.55	삼성전자	1,717
2	케이티	정보통신업	1,035	-	5.41	케이티	1,021
3	쿠팡	도·소매업	639	↑1	6.88	에스케이텔레콤	627
4	에스케이하이닉스	제조업	590	↑1	7.33	쿠팡	535
5	에스케이텔레콤	정보통신업	550	↓2	3.76	에스케이하이닉스	526
6	국민은행	금융·보험업	542	해당없음	8.92	엘지전자	455
7	삼성에스디에스	정보통신업	530	↑13	11.33	우리은행	406
8	엘지전자	제조업	457	↓2	11.71	HD현대중공업	364
9	LG유플러스	정보통신업	442	↑1	4.96	네이버	350
10	네이버	정보통신업	416	↓1	3.80	LG유플러스	292

▲*정보보호 투자액 상위 10대 기업[표=과학기술정보통신부]*

정보보호 투자액, 전담인력 증가 : 지속 상승 중

사이버 공격 대상

https://m.boannews.com/html/detail.html?idx=124626

▲서비스별 주요 기업의 정보보호 투자액 비교[자료=과학기술정보통신부]

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

2. 핵심 기술 및 기업 비밀

- 대기업들은 국가 경제에 중요한 역할을 하는 핵심 기술, 연구 개발 자료, 기업 전략 등 민감한 정보를 다수 보유
- 이러한 정보는 산업 스파이, 국가 배후 해킹 그룹 등에게 매우 중요하며, 탈취 시 막대한 경제적 손실

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

2. 핵심 기술 및 기업 비밀

- 대기업들은 국가 경제에 중요한 역할을 하는 핵심 기술, 연구 개발 자료, 기업 전략 등 민감한 정보를 다수 보유
  - 기술 유출 경로

    - 인력 유출 (경쟁사 이직, 헤드헌팅 업체 이용, 퇴직자)

    - 협력사 이용 (협력 업체 이용, 산업 컨설팅)

    - 내부자료 유출 (전자우편, USB, 외장하드, 클라우드, 사내 시스템 해킹)

사이버 공격 대상

■ 대한민국 IT 대기업이 사이버 공격에 취약한 이유

2. 핵심 기술 및 기업 비밀

- 대기업들은 국가 경제에 중요한 역할을 하는 핵심 기술, 연구 개발 자료, 기업 전략 등 민감한 정보를 다수 보유
  - **인력 유출**
    - **경쟁사 :** 국내 기업의 핵심 인력이 해외(주로 중국) 경쟁사로 이직하면서 기밀 기술을 통째로 넘기는 사례가 빈번
      고액 연봉, 현지 체류 비용, 자녀 교육비 등 파격적인 조건으로 유혹하는 경우가 많다
    - **헤드헌팅 :** 특정 기술을 보유한 인력을 맞춤형으로 물색하여 해외 기업으로 이직을 알선
    - **퇴직자 :** 퇴직 후 경쟁사에 취업하거나, 자체적으로 회사를 설립하여 빼돌린 기술을 활용하는 경우

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

2. 핵심 기술 및 기업 비밀

- 대기업들은 국가 경제에 중요한 역할을 하는 핵심 기술, 연구 개발 자료, 기업 전략 등 민감한 정보를 다수 보유
  - **협력사 이용**
    - **협력업체 공략 :** 대기업은 보안 시스템이 잘 구축되어 있지만, 상대적으로 보안이 취약한 핵심 협력업체를 공략
    - **산학협력 및 기술 컨설팅 위장** : 산학협력이나 기술 컨설팅을 빙자하여 기술 정보를 취득하는 우회 수법도 활용

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

2. 핵심 기술 및 기업 비밀

- 대기업들은 국가 경제에 중요한 역할을 하는 핵심 기술, 연구 개발 자료, 기업 전략 등 민감한 정보를 다수 보유
  - **내부자료 유출**

    - **전자우편, USB, 외장하드, 클라우드** : 내부 직원이 자료를 직접 빼돌리는 가장 흔한 방법

      퇴직 전 또는 재직 중에 이메일, USB, 클라우드 등을 통해 기술 자료를 외부로 반출하는 경우가 많다

    - **사내 시스템 해킹 :** 드물지만 내부 시스템에 침투하여 자료를 탈취하는 경우도 있다

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

2. 핵심 기술 및 기업 비밀

- 대기업들은 국가 경제에 중요한 역할을 하는 핵심 기술, 연구 개발 자료, 기업 전략 등 민감한 정보를 다수 보유
  - **대응 노력**
    - **처벌 강화 및 제도 개선:** 정부는 기술 유출에 대한 처벌을 강화하고, 산업기술 보호법 개정 등을 통해 제도적 미비점을 보완
    - **민관 협력**: 국가정보원, 경찰청, 산업통상자원부 등 정부 기관과 기업들이 협력하여 기술 유출을 막기 위한 방첩 및 보호 활동
    - **기업의 노력:** 각 기업은 인력 관리, 보안 시스템 강화, 내부 통제 등을 통해 기술 유출을 예방하기 위한 노력을 지속

      특히 핵심 인력 이탈 방지 및 퇴직자 관리에 더욱 신경 써야 함

사이버 공격 대상

https://youtu.be/V-noPPae1W0

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

3. 국가 배후 해킹 그룹

- 특히 북한과 같이 조직적이고 전문적인 국가 배후 해킹 그룹들은 한국의 주요 IT 기업들을 지속적으로 노림
- 단순히 금전적 이득을 넘어 국가적 차원의 정보 탈취, 사회 혼란 야기 등을 목표로 매우 정교하고 집요한 공격을 시도

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

4. 구조적인 보안 취약점

- 외부 협력사 및 외주 의존도
  - 대기업은 많은 외부 협력업체와 연동되어 시스템을 운영
  - 문제는 이 협력업체들의 보안 수준이 대기업 본사만큼 높지 않을 수 있다는 점
  - 해커들은 상대적으로 보안이 취약한 협력업체를 통해 대기업 시스템으로 침투하는 공급망 공격을 선호
  - 예 : 대기업 보안 인력의 3분의 1이 외주업체에 의존하고 있어 내부 전문성 강화의 필요성이 제기

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

4. 구조적인 보안 취약점

- 보안 투자 및 인력 문제
  - 정보보호 투자액은 증가하는 추세지만, IT 투자 대비 상대적으로 제자리걸음이라는 지적
  - 숙련된 보안 전문가를 충분히 확보하기 어렵고, 내부 보안 인력의 전문성 강화가 지속적으로 이루어지지 않는다는 문제 제기

사이버 공격 대상

대한민국 IT 대기업이 사이버 공격에 취약한 이유

4. 구조적인 보안 취약점

- 복잡하고 거대한 시스템
  - 대기업의 IT 인프라는 매우 방대하고 복잡
  - 수많은 시스템, 서버, 네트워크, 애플리케이션이 상호 연결되어 있어 모든 취약점을 완벽하게 파악하고 방어하는 것이 매우 중요

사이버 공격 대상

https://youtu.be/k8zOkqexgc8

사이버 공격 대상

https://youtu.be/sX10oKHQer0

사이버 공격 대상

현실적인 보안 과제 및 한계

1. 보안 투자의 한계
2. 인력 부족 및 전문성 격차
3. 레거시 시스템과 신기술 도입의 충돌
4. 내부 인력의 보안 인식 부족

사이버 공격 대상

현실적인 보안 과제 및 한계

1. 보안 투자의 한계

- 기업의 자원은 한정되어 있고, 보안도 그 자원 중 하나일 뿐

  - 보안은 매우 중요. 하지만 모든 기업의 자원은 무한하지 않다. 돈, 시간, 인력… 이 모든 것들이 한정되어 있다

    보안팀은 '우리가 이만큼 투자하면 이만큼 안전해진다!'라는 것을 경영진에게 설득해야 한다. 이게 생각보다 쉽지 않다

사이버 공격 대상

현실적인 보안 과제 및 한계

1. 보안 투자의 한계

- 투자 대비 효율성, 어떻게 증명
  - 보안 투자는 눈에 보이지 않는다.
  - 마케팅에 100억을 투자하면 매출이 오르는 것은 눈에 보인다
  - 하지만 보안에 100억을 투자해서 해킹을 막았다면, ' 아무 일도 일어나지 않은 것 ' 이 결과
  - ‘아무 일도 일어나지 않았다'는 것이 성공이라는 걸 어떻게 증명?
  - 해킹당해서 큰 피해를 입었을 때 '봐라! 미리 투자했어야지!'라고 말하는 건 너무 늦는다.
  - 보안 투자의 가장 큰 딜레마

사이버 공격 대상

현실적인 보안 과제 및 한계

2. 인력 부족 및 전문성 격차

- 보안 인력 부족
  - 사이버 위협은 너무 빨리 진화하는데, 전문가 양성은 시간이 걸린다
  - 해커들은 하루가 다르게 새로운 공격 기법을 만들어 냄
  - 어제는 이 방법으로 뚫렸는데, 오늘은 완전히 다른 방식으로 공격
  - 이런 속도에 맞춰 보안 지식을 업데이트하고, 새로운 기술을 익히는 것이 매우 어렵다
  - 뛰어난 보안 인재는 정말 귀하고, 기업들도 이런 인재를 찾기 위해 애쓴다
  - 하지만 시장에 공급되는 인력은 수요를 따라가지 못하고 있다

사이버 공격 대상

현실적인 보안 과제 및 한계

2. 인력 부족 및 전문성 격차

- 이론 지식만으로는 실제 해킹을 막기 어렵다
  - 대학에서 보안 이론을 아무리 열심히 배워도, 실제 기업의 복잡한 시스템에 적용하고, 실시간으로 발생하는 공격에 대응하는 것은 차원이 다른 문제
  - 실전 경험이 매우 중요
  - 특정 분야(예: 클라우드 보안, AI 보안 등)는 더욱 전문성이 필요해서, 모든 분야의 전문가를 다 갖추기는 불가능
  - 결국 소수의 전문가가 너무 많은 일을 감당해야 하는 상황이 발생하기도 함

사이버 공격 대상

현실적인 보안 과제 및 한계

3. 레거시 시스템과 신기술 도입의 충돌

- 이론 지식만으로는 실제 해킹을 막기 어렵다
  - 오랫동안 사용해 온 시스템은 안정적이지만, 새로운 위협에 취약할 수 있다
  - 이 시스템들은 안정적으로 잘 작동하지만, 문제는 최신 보안 기술이나 패치를 적용하기 어렵다는 점
  - 새로운 기술은 혁신을 가져오지만, 새로운 취약점도 함께 가져올 수 있다
  - 기업들은 경쟁력을 위해 클라우드, AI, IoT, 빅데이터 등 새로운 기술을 끊임없이 도입

    하지만 새로운 기술은 그 자체로 또 다른 보안 위험을 안고 있다
  - 아직 검증되지 않은 취약점이 있을 수 있고, 보안 담당자들도 새로운 기술에 대한 이해가 부족할 수 있다

사이버 공격 대상

현실적인 보안 과제 및 한계

4. 내부 인력의 보안 인식 부족

- 무심코 한 클릭이 기업 전체를 위협
  - 이메일에 첨부된 악성 파일을 무심코 클릭하거나, 출처 불명의 링크를 누르는 단 한 번의 행동이 기업 전체 네트워크를 마비시키거나, 수천만 명의 고객 정보 유출로 이어질 수 있다
  - 대기업은 워낙 많은 사람이 일하기 때문에, 이런 ' 보안 인식 부족 ' 으로 인한 실수가 발생할 확률이 더 높다
  - 보안 부서가 아무리 노력해도 직원 한 명의 실수로 모든 노력이 물거품이 될 수 있다는 것이 가장 무서운 점

보안 투자의 한계, 어떻게 돌파할 것인가?

의사 결정자들의 관점 이해하기

1. 비용 절감 : 불필요한 지출은 없는가?
2. 수익 증대 : 이 투자가 어떻게 매출로 이어지는가?
3. 위험 관리 : 우리 회사의 가장 큰 위험은 무엇이고, 어떻게 줄일 수 있는가?
4. 경쟁 우위 : 경쟁사 대비 어떤 이점을 얻는가?
5. 브랜드 이미지/평판 : 고객 신뢰도와 기업 가치에 미치는 영향
6. 규제 준수 : 법적 문제나 벌금 발생 가능성

보안 투자의 한계, 어떻게 돌파할 것인가?

의사 결정자들의 관점 이해하기

1. 보안 투자를 '비용'이 아닌 '투자'로 포지셔닝 “회사의 미래를 위한 필수적인 투자로 바꾸어 설득”

- 손실 방지를 통한 가치 증명 (ROI - Return on Investment)
  - 지난해 유출된 개인 정보 1건당 평균 피해액은 약 17만원
  - 우리 회사가 100만 명의 고객 정보를 보유하고 있다면, 대규모 유출 시 최대 ????억 원의 직접적인 피해가 발생할 수 있다
  - 여기에 기업 이미지 하락, 고객 이탈, 주가 하락 등의 무형적 손실은 포함되지 않은 금액
  - 이번 보안 시스템 도입에 드는 비용 50억 원은 이러한 잠재적 피해액에 비하면 매우 효율적인 위험 관리 투자다

보안 투자의 한계, 어떻게 돌파할 것인가?

의사 결정자들의 관점 이해하기

1. 보안 투자를 '비용'이 아닌 '투자'로 포지셔닝 “회사의 미래를 위한 필수적인 투자로 바꾸어 설득”

- 경쟁 우위 및 브랜드 이미지 제고
  - **최근 소비자들은 개인 정보 보호에 매우 민감**
  - 보안 사고가 발생한 기업은 고객 이탈이 심화되고 신규 고객 유치가 어려워짐
  - **반대로 ' 보안에 강한 회사 ' 라는 이미지는 고객들에게 큰 신뢰를 주어 경쟁사 대비 차별화된 강점이 됨**
  - **이는 고객 충성도를 높이고, 장기적으로 매출 증대로 이어질 것**
  - **어떤 회사가 있을까요????**

보안 투자의 한계, 어떻게 돌파할 것인가?

의사 결정자들의 관점 이해하기

1. 보안 투자를 '비용'이 아닌 '투자'로 포지셔닝 “회사의 미래를 위한 필수적인 투자로 바꾸어 설득”
   - 경쟁 우위 및 브랜드 이미지 제고
     - **어떤 회사가 있을까요????**

보안 투자의 한계, 어떻게 돌파할 것인가?

https://youtu.be/U2kTesn4Bcs

보안 투자의 한계, 어떻게 돌파할 것인가?

https://youtu.be/zKveATJ2vVU

보안 투자의 한계, 어떻게 돌파할 것인가?

의사 결정자들의 관점 이해하기

1. 보안 투자를 '비용'이 아닌 '투자'로 포지셔닝 “회사의 미래를 위한 필수적인 투자로 바꾸어 설득”

- 효율성 증대 및 운영 비용 절감
  - 수동적인 보안 점검과 대응은 많은 인력과 시간을 소모
  - 이번에 도입하려는 자동화된 보안 솔루션은 반복적인 업무를 줄여 보안 인력의 업무 효율성을 30% 이상 향상시킬 것
  - 이는 장기적으로 인건비 절감 효과를 가져오며, 인력은 더 중요한 전략적 보안 업무에 집중할 수 있게 됨
  - 사고 발생 후 수습 및 복구 과정은 상상 이상의 비용과 시간을 요구
  - 사전 예방적 보안 투자는 사고 발생 확률을 줄여 복구 비용과 시간 손실을 최소화하며, 이는 예측 가능한 비즈니스 운영 환경을 만듬

보안 투자의 한계, 어떻게 돌파할 것인가?

의사 결정자들의 관점 이해하기

2. 설득시 구체적인 접근 전략

- 데이터 기반의 보고 : 추상적인 위험 대신 구체적인 통계, 사례, 예상 피해 금액을 제시
- 명확한 목표 제시 : "무조건 더 안전하게"가 아니라, "이 투자를 통해 어떤 위험을 얼마나 줄일 것인지"를 명확히 함
- **단계별 로드맵 제시 : 한 번에 큰 투자를 요구하기보다, 단기-중기-장기 계획을 제시하여 부담을 줄이고 점진적인 성과를 보여줌**
- 성공 사례 및 벤치마킹 : 유사한 업계의 성공적인 보안 투자 사례나, 경쟁사의 보안 강화 동향을 제시하여 '우리도 해야 한다'는 공감대를 형성(?????)

미래 정보보호 전문가의 역할과 역량

침해 사고 대응 및 복구

- 침해 사고 대응 절차 : 각 단계에서 무엇을 해야 하는지 구체적으로 알고 있어야 함
- 모의 훈련(Table-top Exercise)의 중요성 : 실제 사고와 유사한 상황을 가정하고 시뮬레이션하여 대응 능력을 향상
- 포렌식(Forensic) 및 증거 보전의 중요성 : 법적 대응 및 재발 방지를 위한 침해 흔적 분석 방법
- 커뮤니케이션 전략 : 사고 발생 시 내부 및 외부에 어떻게 정보를 전달하고 소통해야 하는지 (위기 관리 관점)

미래 정보보호 전문가의 역할과 역량

정보보호 전문가의 필수 역량

- 문제 해결 능력 : 복잡한 상황에서 핵심 문제를 파악하고 해결책을 찾아내는 능력
- 분석적 사고 : 방대한 데이터 속에서 의미 있는 패턴을 찾아내는 능력
- 의사소통 능력 : 비기술 직군(경영진, 일반 직원)에게 복잡한 보안 개념을 쉽게 설명하고 설득하는 능력
- 협업 능력 : 개발팀, 운영팀, 법무팀 등 다양한 부서와 협력하는 능력
- 지속적인 학습 능력 : 끊임없이 변화하는 기술과 위협에 발맞춰 스스로 학습하는 자세
- 윤리 의식 : 민감한 정보를 다루는 직업으로서의 높은 윤리 의식과 책임감

프로세스 중심의 프레임워크

- **Computer Crime에 대응 하기 위해 실무적인 방법론으로 2001년 Prosise등이 제시**
  - 컴퓨터 범죄(computer crime)에 대응하기 위한 **실무적 방법론을 제시한 이유는 그 당시 급속히 확산되는 사이버 범죄와 해킹 위협에 효과적으로 대응할 필요가 있었기 때문**
  - **2000년대 초반은 인터넷과 컴퓨터 기술이 전 세계적으로 급격히 확산되면서 컴퓨터 범죄가 크게 증가한 시기**
  - 특히 해킹, 바이러스와 같은 다양한 형태의 사이버 공격이 등장하면서 정보 보안에 대한 위협이 커짐
  - 컴퓨터 범죄의 '양적 팽창'과 '질적 진화'가 동시에 이루어진 시기
  - '사이버 보안'이라는 개념의 중요성을 일깨우는 계기

컴퓨터 범죄 대응의 실무적 방법론

- **Computer Crime에 대응 하기 위해 실무적인 방법론으로 2001년 Prosise등이 제시**
  - **당시에는 컴퓨터 범죄와 관련된 표준화된 대응 방법론이나 법적 기준이 부족**
  - 사건이 발생했을 때 어떻게 대처할지에 대한 체계적인 접근 방식이 필요
  - **컴퓨터 범죄 대응에 필요한 실무적인 단계를 구체화함으로써, 컴퓨터 범죄 조사자들이 보다 일관되고 신속하게 대응할 수 있도록 했다**
  - **디지털 증거의 수집, 분석, 보존 및 보고에 중점을 두고, 법적 절차에서 유효하게 사용할 수 있는 증거를 확보하는 방법을 제시**

컴퓨터 범죄 대응의 실무적 방법론

- **Computer Crime에 대응 하기 위해 실무적인 방법론으로 2001년 Prosise등이 제시**

1. 사전 준비 (Pre-Incident Preparation)
2. 사건 탐지 (Detection of Incidents)
3. 초기 대응 (Initial Response)
4. 대응 전략 수립 (Response Strategy Formulation)
5. 데이터 복제 (Duplication)
6. 보안 조치 시행 (Investigation Security Measure Implementation)
7. 네트워크 모니터링 (Network Monitoring)
8. 복구 (Recovery)
9. 보고 및 후속 조치 (Reporting and Follow-Up)

컴퓨터 범죄 대응의 실무적 방법론

사전 준비 (Pre-Incident Preparation)

- 사고는 언제든 발생할 수 있다는 전제 하에 미리 준비하는 단계
  - 침해 사고 대응팀 구성: 누가 어떤 역할을 할 것인가? (예: 기술 분석가, 법률 전문가, 홍보 담당자 등)
  - 대응 절차 및 매뉴얼 구축: 사고 유형별(랜섬웨어, DDoS, 정보 유출 등) 대응 절차 문서화.
  - 필수 도구 준비: 포렌식 도구, 네트워크 모니터링, 백업 시스템, 안전한 통신 채널 등.
  - 훈련 및 모의 훈련: 정기적인 훈련으로 팀원들의 역량 강화 및 매뉴얼 검증.
  - 법적/규제적 요건 이해: 사고 발생 시 보고 의무, 증거 보전 원칙 등 미리 숙지.

컴퓨터 범죄 대응의 실무적 방법론

사전 준비 (Pre-Incident Preparation)

- 사고는 언제든 발생할 수 있다는 전제 하에 미리 준비하는 단계
  - 법적/규제적 요건 이해: 사고 발생 시 보고 의무, 증거 보전 원칙 등 미리 숙지.
    - **침해 사고 '보고 의무' 이해**
    - 우리나라의 정보보호 관련 법규는 기업이나 기관에서 개인 정보 유출이나 심각한 정보보호 침해 사고가 발생했을 때, 이를 관계 당국에 의무적으로 보고하도록 규정
    - 개인정보보호법 : 개인정보처리자 (개인정보를 처리하는 모든 공공기관, 법인, 단체 및 개인)
    - 개인정보 유출 사실 인지 시: 즉시(24시간 이내) 과학기술정보통신부(KISA) 또는 개인정보보호위원회에 신고
    - 정보주체(피해자) 통지: 유출 사실을 해당 정보주체에게 지체 없이 알려야 함

컴퓨터 범죄 대응의 실무적 방법론

사전 준비 (Pre-Incident Preparation)

- 사고는 언제든 발생할 수 있다는 전제 하에 미리 준비하는 단계
  - 법적/규제적 요건 이해: 사고 발생 시 보고 의무, 증거 보전 원칙 등 미리 숙지.
    - **정보통신망 이용촉진 및 정보보호 등에 관한 법률 (정보통신망법)**
    - 대상: 정보통신서비스 제공자 (ISP, 포털, 통신사 등)
    - 침해사고 발생 시: 과학기술정보통신부 장관(KISA)에게 지체 없이 신고해야 함

컴퓨터 범죄 대응의 실무적 방법론

사전 준비 (Pre-Incident Preparation)

- 사고는 언제든 발생할 수 있다는 전제 하에 미리 준비하는 단계
  - 법적/규제적 요건 이해: 사고 발생 시 보고 의무, 증거 보전 원칙 등 미리 숙지.
    - **증거보존**

      - 침해된 서버/PC의 디스크 이미지 (포렌식 이미지)

      - 네트워크 패킷 캡처 파일

      - 각종 시스템 로그 (웹 서버 로그, OS 로그, DB 로그, 방화벽 로그 등)

      - 메모리 덤프

      - 악성코드 샘플

      - 관련 이메일, 문서 등

컴퓨터 범죄 대응의 실무적 방법론

사건 탐지 (Detection of Incidents)

- 이상 징후를 빠르게 인지하고 사고로 판단하는 단계.
  - 다양한 탐지 원천: 방화벽 로그, 웹로그, 사용자 신고, 외부 제보 등.
  - 오탐(False Positive)과 미탐(False Negative): 오탐이 많으면 피로도가 높아지고, 미탐은 실제 공격을 놓치는 것임을 강조.
    - 오탐 : 실제로 위협이 아닌 것을 위협으로 잘못 탐지
    - 미탐 : 실제로 위협인 것을 위협으로 탐지하지 못하고 놓치는 것
  - 정확한 알림 설정: 중요도에 따른 알림 기준 설정 및 신속한 전달 체계.
  - 최신 위협 인텔리전스 활용: 새로운 공격 패턴을 미리 파악하고 탐지 룰에 반영.

컴퓨터 범죄 대응의 실무적 방법론

사건 탐지 (Detection of Incidents)

- 어떤 징후들을 보고, 공격당하고 있나를 알 수 있을까요?
  - 네트워크 트래픽의 비정상적인 변화
    - 급증하는 특정 트래픽 : 평소보다 특정 포트(예: 웹 서비스 80 포트)나 특정 목적지(예: 해외 특정 IP)로 나가는 트래픽이 비정상적으로 많다면 DDoS 공격이나 내부 시스템에서 외부로의 데이터 유출을 의심
    - 특정 시간대의 비정상적인 접속: 근무 시간이 아닌 새벽 시간대에 외부에서 내부 시스템으로 접속 시도가 많거나, 평소 사용하지 않던 프로토콜 트래픽이 감지될 때

컴퓨터 범죄 대응의 실무적 방법론

사건 탐지 (Detection of Incidents)

- 어떤 징후들을 보고, 공격당하고 있나를 알 수 있을까요?
  - 시스템 및 서버의 비정상적인 동작:
    - CPU/메모리 사용량 급증: 평소보다 서버의 CPU나 메모리 사용량이 갑자기 치솟는다면 악성코드 감염이나 과도한 프로세스 실행, DDoS 공격 등을 의심
    - 디스크 공간 급감: 랜섬웨어 감염으로 암호화된 파일이 늘어나거나, 대량의 로그가 생성될 때 디스크 공간이 빠르게 줄어들 수 있다
    - 불필요한 프로세스 실행: 관리자가 설치하지 않은 의심스러운 프로세스나 서비스가 백그라운드에서 실행될 때.

컴퓨터 범죄 대응의 실무적 방법론

사건 탐지 (Detection of Incidents)

- 어떤 징후들을 보고, 공격당하고 있나를 알 수 있을까요?
  - 로그 파일의 이상 징후:
    - 로그인 실패 기록 급증: 특정 계정으로의 로그인 실패 시도가 반복된다면 무작위 대입(Brute-force) 공격을 의심할 수 있다
    - 비정상적인 로그인 시도: 관리자가 아닌 계정으로 관리자 권한을 획득하려는 시도, 해외 IP에서의 로그인 시도.
    - 방화벽 경고: 보안 장비에서 악성 IP 접근 차단, 침입 탐지 등의 경고가 다수 발생할 때.

컴퓨터 범죄 대응의 실무적 방법론

초기 대응 (Initial Response)

- 탐지된 사고에 대해 즉각적이고 제한적인 조치를 취하는 단계.
  - 사고 범위 확인: 침해된 시스템, 데이터, 계정은 무엇이며, 얼마나 광범위한가?
  - 격리(Containment) 전략: 추가 확산을 막기 위해 네트워크 단절, 시스템 종료, 계정 잠금 등. (예: "랜섬웨어 감염 시 해당 PC를 즉시 네트워크에서 분리하는 것이 중요합니다.")
  - 초기 정보 수집: 어떤 공격인지, 어떻게 침투했는지 등 기본적인 정보 파악.
  - 경영진 및 관련 부서 통보: 상황 공유 및 초기 판단.

컴퓨터 범죄 대응의 실무적 방법론

대응 전략 수립 (Response Strategy Formulation)

- 수집된 정보를 바탕으로 향후 대응 방향을 결정하는 단계
  - **피해 분석 및 영향 평가:** 비즈니스에 미치는 영향(재정적, 평판적, 운영적)을 심층적으로 분석.
  - **목표 설정**: 이번 사고 대응의 최종 목표는 무엇인가? (예: "데이터 유출 확인 및 복구", "시스템 완전 정상화", "공격자 추적")
  - **자원 배분**: 인력, 예산, 외부 전문가 지원 등 필요한 자원 할당.
  - **법률 및 규제 전문가 협력:** 법적 대응 방안 논의 (수사 의뢰 여부, 피해 고지 등).
  - **커뮤니케이션 계획:** 내부 직원, 고객, 언론 등과의 소통 계획 수립.

컴퓨터 범죄 대응의 실무적 방법론

데이터 복제 (Duplication)

- 추가 분석 및 법적 증거를 위해 원본(감염됨) 데이터를 안전하게 복제하는 단계
  - 포렌식 이미지 생성: 물리적 드라이브나 메모리 복제(훼손 방지).
  - 무결성 확보: 해시 값(MD5, SHA-256)을 이용하여 복제된 데이터가 원본과 동일함을 증명.
  - 증거 유지: 누가 언제 어떤 데이터를 어떻게 다루었는지 기록하고 보존.
  - 안전한 보관: 복제된 증거 데이터를 안전하게 보관하는 방법.

컴퓨터 범죄 대응의 실무적 방법론

보안 조치 시행 (Investigation Security Measure Implementation)

- 원인 파악 및 추가 공격 방지를 위한 보안 조치를 실행하는 단계
  - 취약점 분석 및 패치: 침투 경로로 사용된 취약점을 찾아내고 즉시 패치.
  - 악성코드 제거: 시스템 내부에 잔존하는 악성코드를 탐지하고 제거.
  - 권한 및 계정 재설정: 유출된 계정의 비밀번호 변경, 불필요한 권한 제거.
  - 재발 방지 시스템 강화: 침투에 사용된 기술에 대응할 수 있는 보안 시스템(방화벽 룰 등) 강화.
  - 로그 분석: 침해된 시스템의 로그를 분석하여 공격의 전개 과정 상세 파악.

컴퓨터 범죄 대응의 실무적 방법론

네트워크 모니터링 (Network Monitoring)

- 사고 조치 후 재발 여부를 감시하고, 공격자의 잔존 여부를 확인하는 단계.
  - 비정상적인 트래픽 감시: 평소와 다른 네트워크 흐름, 외부와의 수상한 통신 여부.
  - 내부 시스템 비정상 행위 탐지: 숨겨진 백도어, 의심스러운 파일 생성, 권한 상승 시도 등.
  - 보안 장비 로그 실시간 분석: 방화벽 등에서 발생하는 경고 실시간 확인.

컴퓨터 범죄 대응의 실무적 방법론

복구 (Recovery)

- **침해로 인해 손상된 시스템과 데이터를 정상 상태로 되돌리는 단계.**

  - (백업 룰이 시행이 되고 있을 것, (주기적)), 물리적으로도 백업이 되고 있을 것 (천재지변 대비)

- **안전한 백업 데이터 복원:** 사고 발생 이전의 안전한 시점으로 데이터 복구.
- **손상된 시스템 재구축/정비: 오염되거나 손상된 시스템을 깨끗하게 재설치 또는 정비.**
- **서비스 재개: 고객에게 서비스 재개 시점 및 정상 운영 알림.**
- **완전성 및 무결성 확인: 복구된 데이터와 시스템이 손상되지 않고 완전한지 검증.**

컴퓨터 범죄 대응의 실무적 방법론

보고 및 후속 조치 (Reporting and Follow-Up)

- **사고의 전말을 분석하고, 재발 방지를 위한 개선 사항을 도출하는 단계.**
  - 사고 보고서 작성: 사고의 원인, 대응 과정, 피해 규모, 재발 방지 대책 등을 상세히 기록. (기술적 보고서, 경영진 보고서 등 목적에 따라 다르게 작성).
  - Lessons Learned (교훈 도출): 무엇이 잘 되었고, 무엇이 부족했으며, 다음에는 어떻게 개선할 것인지 논의.
  - 보안 정책 및 절차 업데이트: 사고를 통해 드러난 약점을 보완하기 위해 기존 정책 및 절차 개선.
  - 시스템 및 인프라 개선: 취약점을 근본적으로 해결하기 위한 시스템 업그레이드 또는 재설계.
  - **정기적인 감사 및 검토: 개선 사항이 잘 적용되고 있는지 주기적으로 확인.**

통합적 보안 관점의 중요성

보안은 더 이상 개별적인 영역이 아니라 모든 것이 연결된 복합적인 시스템

- **보안은 개발팀, 운영팀, 법무팀, 홍보팀, 심지어 경영진까지 모든 부서가 함께 움직여야 함**
  - **협업의 중요성:** 개발 단계부터 보안을 고려, 운영 단계에서 보안팀과 IT 운영팀의 긴밀한 협력, 사고 발생 시 법무팀과의 소통, 언론 대응을 위한 홍보팀과의 조율 등.
  - **보안 문화 확산:** 모든 임직원이 보안을 '내 일'로 인식하도록 하는 교육과 캠페인의 중요성, 단순히 지식 전달을 넘어 보안을 습관화하는 문화가 필요
  - **외부 협력의 필요성:** 보안 솔루션 벤더, 보안 컨설팅 업체, 정부 기관(KISA 등)과의 협력 체계 구축

침해 사고 대응 연습

Tabletop Exercise (토론 기반 훈련)

- Tabletop Exercise는 말 그대로 '테이블 위에서' 진행하는 훈련
- 실제 시스템이나 장비를 사용하지 않고, 미리 준비된 '가상의 시나리오'를 바탕으로 사고 대응팀 구성원들이 한자리에 모여 토론
- 사고에 대응하는 과정을 연습
  - '이런 상황이라면 우리가 무엇을 해야 할까?'
  - '다음 단계는 무엇이지?' 하고 서로 토론

침해 사고 대응 연습

Tabletop Exercise (토론 기반 훈련) - 중요성

- 숨겨진 문제점 발견
  - 아무리 잘 만들어진 침해 사고 대응 매뉴얼도 실제 상황에서 100% 완벽할 수는 없다
  - 매뉴얼에 명시되지 않은 애매한 부분,
  - 여러 부서 간 역할이 겹치거나 비어있는 부분,
  - 미처 예상하지 못했던 상황 발생 시 어떤 식으로 대응해야 할지 막연했던 부분들을 찾아 낼 수 있다

침해 사고 대응 연습

Tabletop Exercise (토론 기반 훈련) - 중요성

- 팀워크와 의사소통 강화
  - 사고 상황에서는 모든 것이 급박
  - 각자의 역할과 책임이 명확하지 않거나, 소통이 원활하지 않으면 대응이 늦어지고 피해가 커질 수 있다
  - 팀원들이 서로의 역할을 이해하고, 위기 상황에서 어떻게 정보를 공유하고 의사결정을 내려야 하는지를 연습하는 좋은 기회

침해 사고 대응 연습

Tabletop Exercise (토론 기반 훈련) - 중요성

- 비용 및 시간 효율성
  - 실제 시스템을 동원하거나 공격을 시뮬레이션하는 Full-Scale Exercise는 엄청난 비용과 시간이 소요
  - Tabletop Exercise는 비교적 적은 비용과 짧은 시간에 많은 사람들을 참여시켜 효과적인 훈련을 진행할 수 있다
  - 조직의 모든 핵심 인력이 참여하여 토론하는 것이 중요

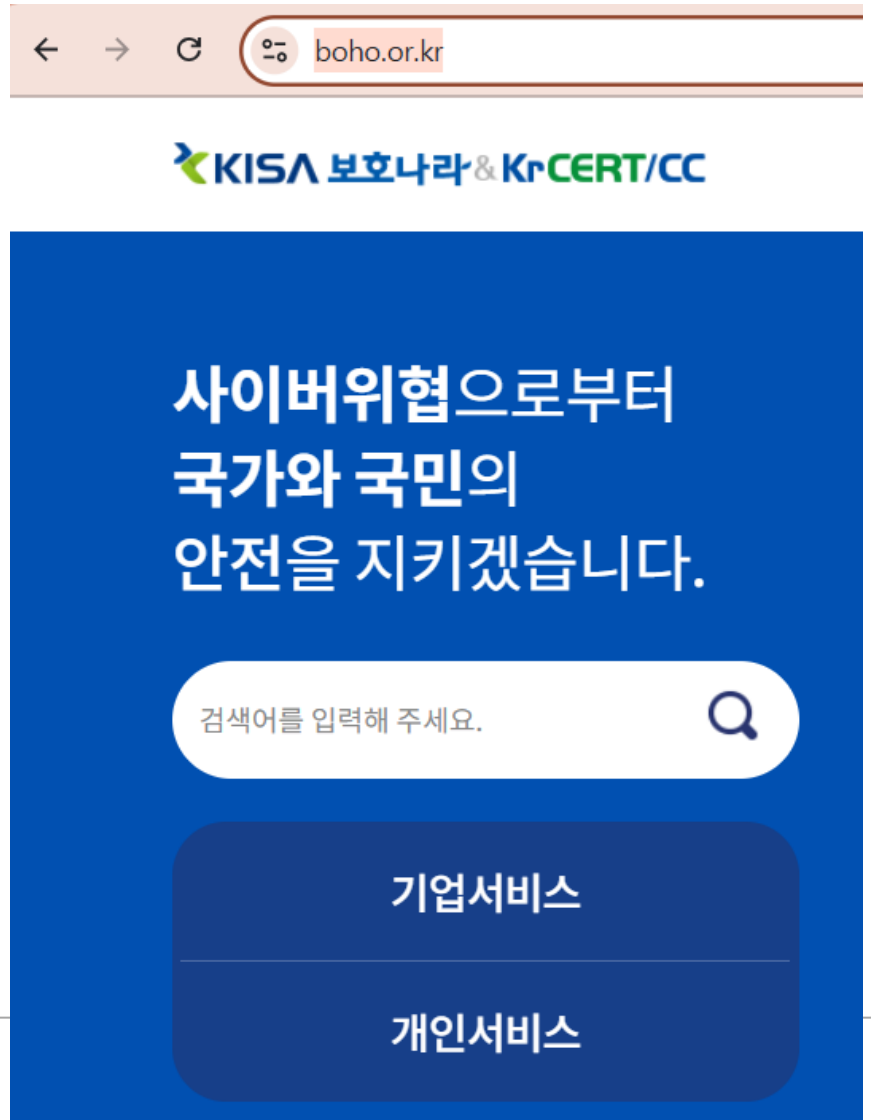
침해 사고 대응 연습

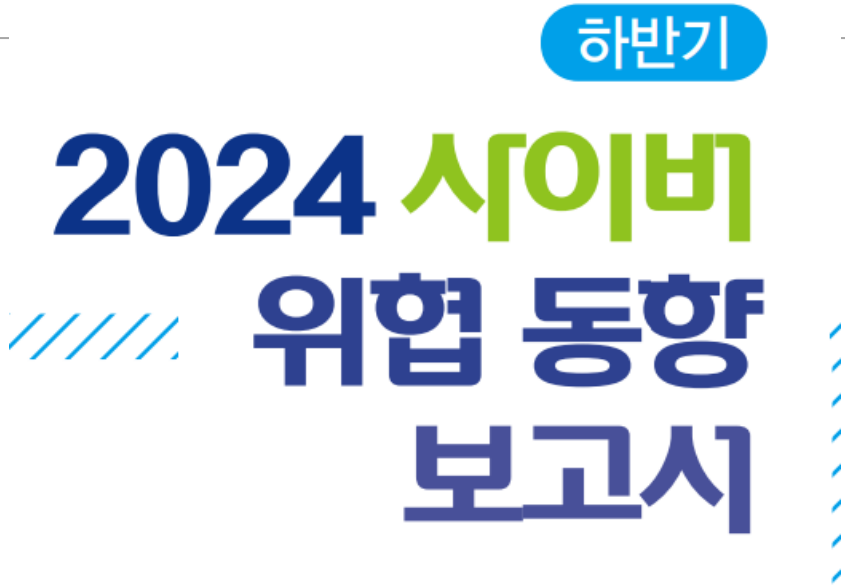
실제 침해 사고 케이스 스터디 (Case Study)

- 타 기업에서 실제로 발생했던 침해 사고 사례를 분석하는 것은 매우 중요한 학습 방법
- 다른 기업의 실패와 성공 경험을 통해 우리는 많은 것을 배울 수 있다
  - 침투 경로: 어떤 취약점이 악용되었는가? (기술적 측면)
  - 피해 확산 과정: 왜 피해가 커졌는가? (대응 초기 미흡, 내부 시스템 연동 문제 등)
  - 대응 과정: 어떤 조치가 효과적이었고, 어떤 부분에서 아쉬웠는가? (Prosise 모델의 각 단계에 대입하여 분석)
  - 법적/사회적 파장: 기업 이미지, 주가, 법적 소송 등 비즈니스에 미친 영향.
  - 재발 방지 대책: 해당 기업이 이후 어떤 보안 강화 조치를 취했는가?
  - 강조할 점: 다른 기업의 사례를 '남의 일'이라고 생각하지 말고, '우리 회사라면 어떻게 되었을까?', '나는 어떻게 대응했을까?'라는 관점에서 비판적으로 분석하는 것이 중요

기타

https://www.boho.or.kr/





기타

표 1 – 2 유형별 침해사고 신고 현황

[단위 : 건수]

구분 \ 연도		2023 (상반기)	비율	2023 (하반기)	비율	2024 (상반기)	비율	2024 (하반기)	비율
침해사고 신고	DDoS 공격	124	18.7%	89	14.5%	153	17.0%	132	13.4%
	악성코드	156	23.5%	144	23.5%	106	11.8%	123	12.4%
	(랜섬웨어)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)	(103)	(10.4%)
	서버 해킹	320	48.2%	263	42.9%	504	56.1%	553	56.0%
	기타	64	9.6%	117	19.1%	136	15.1%	180	18.2%
합 계		664		613		899		988	

기타

표 1 – 3 업종별 침해사고 신고 현황

[단위 : 건수]

구분 \ 연도	2022 (하반기)	비율	2022 (하반기)	비율	2023 (하반기)	비율	2024 (하반기)	비율
정보통신업	250	37.7%	192	31.3%	302	33.6%	299	30.3%
제조업	130	19.6%	115	18.8%	147	16.4%	186	18.8%
도매 및 소매업	95	14.3%	89	14.5%	126	14.0%	134	13.6%
협회 및 단체, 수리 및 기타 개인 서비스업	39	5.9%	34	5.5%	47	5.2%	74	7.5%
기타	150	22.6%	183	29.9%	277	31.0%	295	29.9%
합 계	664		613		899		988	

기타

https://youtu.be/8IEUKMMTfJg

Thank you for Listening

새로운 세상과 변화에 도전하는 동국대인이 되기를 바랍니다.