DCS
Daejeon Chungnam Sejong
대학원격교육지원센터

안녕하십니까? 대전·충남·세종 권역 대학원격교육지원센터입니다.

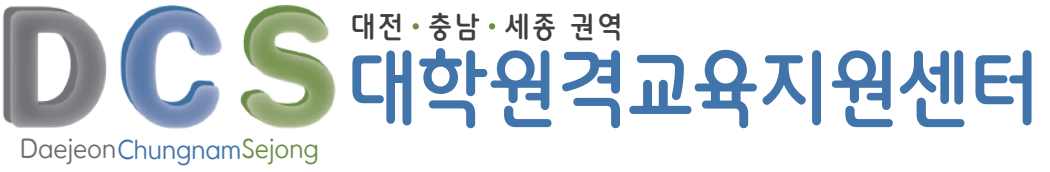
대전·충남·세종 권역 대학원격교육지원센터는 권역 내 대학·전문대학을 연계하고 지원하며 디지털 기반 미래교육 혁신을 위한 원격교육 생태계를 구축 및 지원하고 있습니다.

<DCS Together>에서는 원격수업 혁신을 위한 지원의 일환으로 최신 교수법 동향, 수업노하우, 정책연구 결과, 대전·충남·세종 권역 대학원격교육지원센터 설치 운영사업에 대한 홍보를 제공하고 있습니다.

더불어 권역 내 공동활용 가능한 강의녹화 스튜디오를 충남대학교, 대전과학기술대학교에 구축하여 운영하고 있으며, 공동활용이 가능한 원격강의 콘텐츠를 개발 및 공유하고 있으니 많은 관심 부탁드립니다.

DCS 대전·충남·세종 권역 대학원격교육지원센터 University Distance Education Center
Daejeon Chungnam Sejong
• 주소 : 34134 대전광역시 유성구 대학로99, 충남대학교 중앙도서관 1층
• TEL : 042-821-6068 • E-mail : cyberdcs@cnu.ac.kr
• https://udec.cnu.ac.kr

온라인 전환으로 대학교들의 사이버 보안 취약성이 확대됨



온라인 전환으로 대학교들의 사이버 보안 취약성이 확대됨[1]

2019년부터 2020년까지 랜섬웨어 공격은 두 배로 증가했으며, 전문가들은 온라인 학습의 증가로 인해 대학교들이 새로운 위협에 직면해 있다고 경고함. 캠퍼스 기능의 다양화로 인해 포괄적인 보안 프로그램을 구축하기가 어렵고, 교육 기관은 또한 방대한 수의 디지털 개인정보를 보유하고 있어 해커에게 주요 표적이 됨. 대학교들은 노후화 된 IT 인프라로 인해 데이터를 안전하게 저장하거나 전송하기 어려우며 이것이 상황을 복잡하게 만들고 있음.

I 온라인 전환으로 랜섬웨어 공격이 두 배로 증가함

- "고등 교육에서의 사이버 보안" 보고서에 따르면, 컴퓨터의 작동이 중단되게 만든 뒤 재가동을 조건으로 금품을 요구하는 악성프로그램의 일종인 랜섬웨어 공격은 2019년~2020년 기간 동안 두 배로 증가했으며 전문가들은 온라인 학습의 증가로 인해 대학교들이 새로운 위협에 직면해 있다고 경고함.
- 랜섬웨어 유포 초기인 2010년, 오하이오 주립대학이 공격을 받았으며 학교와 관련된 70만 명 이상의 개인정보가 이에 영향을 받았음. 개인정보가 실제로 도난당했다는 증거는 없었지만, 이 사건은 오하이오 주와 다른 주요 대학에 랜섬웨어에 대한 경각심을 일으켰음. 당시에는 랜섬웨어에 의한 공격은 새로운 위협이었으며, 지난 10년 동안 대학들은 이러한 위험에 보다 적극적으로 대처함.

대학교가 사이버 범죄의 표적이 되는 이유

- IT 컨설팅 회사인 Tambellini Group의 연구 부사장인 Dave Kieffer는 사이버 범죄자들이 대학을 표적으로 삼고 있는 이유로, 대학교 기능의 다양성으로 인해 포괄적인 보안 프로그램을 구축하기가 어렵고, 교육 기관은 또한 방대한 수의 디지털 개인정보를 보유하고 있어 해커에게 보물 창고로 여겨진다는 점을 가리킴. 연구 중심 대학교의 지적 재산도 점점 더 표적이 되고 있으며, 대학교에서 흔히 볼 수 있는 노후 IT 인프라는 데이터를 안전하게 저장하거나 전송하기 어렵게 만들어 상황을 복잡하게 만들고 있음.
- 코로나19로 인해 지난봄에 대부분의 대학교가 수업과 활동의 대부분을 온라인으로 전환했을 때, 위에서 언급한 여러 종류의 취약성으로 인해 사이버 보안 위험 수준이 높아짐. 학생과 교직원이 전 세계에 분산되어 있어 보안 시스템 유지가 불필요해 보일 수 있지만, 온라인 학습 증가로 인한 새로운 위협의 증가로 사이버 보안 시스템을 유지해야 함.

1 https://www.highereddive.com/news/shift-online-exposed-and-expanded-college-cybersecurity-vulnerabilities/597451/ (Education Dive, 2021.3.30) 〈Keyword〉 사이버 보안, 원격 교육, 개인정보, 온라인 수업

Ⅱ 팬데믹 시대의 보안 위험

- 팬데믹이 시작되기 전, 오레곤 Mt. Hood Community College의 교직원들은 주로 대학에서 제공하는 사무기기들을 사용했지만, 코로나19 발생 이후 대부분의 직원이 집에서 일하기 시작하면서 더 많은 개인용 노트북, 태블릿, 전화를 사용하여 업무를 수행해야 했음. 직원들은 원격 작업으로 전환하는 동안 가상 사설망(VPN) 연결을 통해 대학의 내부 시스템에 접근해야 했기 때문에 많은 어려움을 겪었음.
- 대학 네트워크에 대한 가장 큰 위험 중 두 가지는 보안이 되지 않는 와이파이 연결과 로그인 정보를 도난당하기 쉬운 관리 시스템임. VPN 사용은 보안 연결의 필요성을 해결했지만, 안전한 로그인 설정을 하는 것이 더 어려웠음. Mt. Hood Community College는 직원들에게는 새로운 다단계 인증 솔루션을 출시했음. 직원들은 로그인을 하려면 암호와 문자 메시지(SMS)를 통해 전달된 코드 등의 두 가지 이상의 정보를 입력해야 했음.
- 또한 대학교들은 Windows XP 또는 Windows 7과 같은 패치 및 업데이트가 지원되지 않는 소프트웨어와 운영 체제의 사용으로 인해 보안이 더 취약해졌으며, 이는 랜섬웨어 공격의 원인이 되고 있음. 최근 보고서에 따르면 고등교육 기관에 대한 랜섬웨어 공격은 2019년~2020년 기간 동안 두 배로 증가하여 평균 447,000 달러의 손실이 발생함. 이 보고서는 랜섬웨어 공격이 대학의 가장 큰 사이버 위협라고 경고함.
- 대부분의 랜섬웨어 공격은 피싱으로 시작됨. 피싱은 범죄자가 사용자의 이메일, SMS 및 소셜미디어를 통해 악성 링크를 보내고, 사용자가 링크를 클릭하거나 피싱 이메일의 첨부 파일을 열면 악성소프트웨어가 다운로드 되거나 로그인 정보가 노출됨.
- 최근 몇 년 동안 대학교들은 집중적으로 데이터 유출을 겪었음. 팬데믹 이후 시작된 원격교육 등, 학습 및 일상 업무에 사용된 기술들은 사이버 범죄자들에게 새로운 기회를 열어주었고, 학교들은 사이버 공격에 더욱 취약해졌음. 원격학습과 원격업무의 보편화는, 보안이 되지 않은 네트워크를 통해 민감한 정보가 노출되거나, 권한이 없는 사람들이 민감한 정보를 공유할 수 있는 계기가 됨. 데이터 유출은 악의를 가진 외부인에 의해서만 발생하는 것이 아니라, 암호화되지 않은 이메일로 학생 기록이 포함된 스프레드시트를 전송하는 등 개인정보 보안 규칙을 위반하는 내부자에 의해 발생하기도 함.

Ⅲ 사이버 공격의 위협을 감소시키는 방법

- 사이버 공격은 대학과 개인정보가 노출될 수 있는 학생과 교직원들에게 많은 손실을 가져옴. 교육기관들이 온라인 수업에 더 많이 의존함에 따라, 보안을 개선하려면 학교는 다음 사항을 고려해야함.
  - ➤ 대학은 개인정보 노출 등 보안사고 발생에 대한 책임을 져야하며, 대학교 총장과 이사회가 관심을 갖고 사이버 보안과 위험에 대해 관리해야 함.
  - ➤ IT 예산은 소프트웨어, 하드웨어 및 네트워크 업그레이드를 지속적으로 고려하여 편성해야 함.
  - ➤ 서로 연결되지 않은 대학교 인트라넷으로 인해 한 사람이 여러 개의 ID를 갖게 됨. ID 수를 줄이기 위해 네트워크 통합을 고려하고 ID와 접근관리 시스템을 구축해야 함.

- 모든 네트워크 연결에 다단계 인증이 필요하며, 이를 통해 보안을 강화해야 함.
- IT 및 보안 담당자들이 보유하고 있는 정보의 위치, 이동 방법 등 내부 데이터를 더 잘 이해할 수 있게 해주는 정보관리 프로그램을 사용해야 함. 정보에 관해 더 많이 알수록 더 잘 보호 할 수 있음.
- 인트라넷에 연결되지 않은 데이터 백업 시스템을 설치해야 함. 랜섬웨어 공격이 있는 경우 백업을 사용하여 작업을 계속 실행할 수 있음.
- 대부분의 학생들은 컴퓨터와 함께 자랐으며 개인정보 보호 및 보안문제에 민감하지 않을 수 있음. 모든 학생은 물론 교직원에게 보안의 중요성을 인식시키기 위한 교육이 필요함.