2011년 5월 18일 키워드 스피킹 방송 / 주제: 사이버보안 및 해킹

Paul's Summary (transcribed)

As the world becomes more connected, more and more services are being brought online. Despite claims from companies that cyberspace is more secure than ever, recent events have **casted doubt**.

Both Nonghyup Bank (NH) and Hyundai Capital had been **victims of hacking** these past few weeks. Nonghyup claimed that North Korea had **made a cyber attack on** their online banking system that **paralyzed** millions of accounts for weeks. They concluded along with the Korean National Intelligence Service that North Korea's intelligence agency called the Reconnaissance General Bureau (RGB) was **to blame** for the **breakdown in security**. It has been reported that the RGB has more than a thousand hackers working to **disrupt** vital South Korean networks such as online banks, subways, airports, and telecommunications facilities.

Other critics claim that NH bank is trying to **evade responsibility** by sensationalizing claims of cyber terrorism without proper evidence. It is true that an **IBM subcontractor's laptop** was **turned into a zombie computer** that deleted critical files on NH Bank servers. And that the original attacker's IP address was similar to the one used when NH networks were attacked back in 2009. But this doesn't clearly prove that North Korea is to blame. What is more apparent is that NH had been managing their online system **in a sloppy and amateurish way** by not changing their passwords for more than six years. Hyundai Capital's attack was carried out by South Koreans who tried to **blackmail** the financial firm out of almost half a million dollars. Two out of the three criminals were caught which shows that even a few amateurs could **break into the networks** of the most prestigious companies.

It's not only Korea that is having trouble with cyber attacks. Last month Japan's Playstation Network had been **hacked** causing weeks of unavailable service along with the theft of tens of millions of customer credit cards. It seems that there will never be a lock that can't be picked, a vault that isn't breakable, or even a firewall that can't be hacked.

Key Words

1. 사이버 보안 cyber security
2. 해킹에 취약하다 vulnerable to hacking
3. 전산망 마비 network breakdown, disruption of the network, network paralysis
4. 관리허술 do a sloppy job of maintaining security, neglectful of their duty, have negligence
5. 북한 소행 North Korea is held responsible, North Korea is to blame
6. 악성코드를 심다 plant malware into your computer, plant virus, install malware
7. 좀비pc를 만들다 turn your computer into a zombie computer
8. 해킹당하다 be hacked, be hacked into
9. 사이버 공격 cyber attacks
10. 보안불감증 security personnel have negligence, neglectful of their duty
11. 암호화 encryption, be encrypted
12. 개인정보 유출 leakage of personal information, personal information was leaked
13. 소 잃고 외양간 고친다 Don't close the barn door after the horse runs away; You fix the barn after the cow broke away; you should have taken care of it when you had the chance

More Key Words

1. 컴퓨터를 잘 아는 computer savvy
2. 알려지지 않은 사이트 unreputable websites, suspicious websites
3. 백신프로그램을 설치하다 install anti-virus program
4. 의심을 해보다 cast doubt
5. 책임을 회피하다 evade responsibility
6. IBM 협력사 직원의 노트북 IBM subcontractor's laptop
7. 아마추어처럼 허술하게 in a sloppy and amateurish way

8. 협박하다 blackmail