Reading: IT security and the human element
Technical English for IN/IT

Stop worrying about mastermind hackers. Start worrying about the IT guy.

Mistakes in setting up popular office software have sent information about millions of Americans spilling onto the Internet, including Social Security numbers of college students, the names of children in Texas and the ID numbers of intelligence officials who visited a port facility in Maryland.

The security problem, researchers say, has affected many hundreds of servers running Oracle software. Most of the institutions affected have been universities or government agencies, which hold a wide range of information on individuals and private companies.

The UCLA Health system, for example, had communications records — including doctors's names, email addresses and phone numbers — visible online. The Texas State Department of Family and Protective Services left the names, birth dates and other information about children exposed to the Internet. At the Port of Baltimore, logs of visitors were left vulnerable, which included information about foreign diplomats, State Department employees and officials from the Defense Intelligence Agency.

This was not the work of sophisticated Russian hackers or Chinese cyber-warriors, who typically get blamed for problems in computer networks. Instead, researchers are pointing to humble system administrators for making routine errors that left the data unsecured.

The scale of the mix-up has highlighted how in an era of soaring national investment in cyber-security, the weakest link often involves the inherent fallibility of humans. Experts say even the most skilled system administrators struggle to keep every computer at large institutions running smoothly, with the proper software updates, security patches and configurations.

Steven Bellovin, a professor of computer science at Columbia University, said, “Some systems are just impossible to configure correctly. The code is complex.”

Ben Caudill of Rhino Security Labs added, “I would suspect that each one of these organizations have dozens or more routers and switches that manage which systems are connected to the Internet and which ports are exposed. A lot of times, organizations don't really know what's publicly accessible, and that becomes a real big problem.”

Flaws in Oracle's Reports software were discovered in 2011 and reported to the company. Oracle began warning customers and issuing patches to solve the problem in 2012. Yet even two years later, anyone with an Internet connection and knowledge of certain Oracle software commands can download sensitive information from servers running affected — but unpatched — software.

Some experts lay at least some of the blame on Oracle for issuing software that was both complicated to use properly and had default settings that left security weak. If a software patch must be issued to correct a problem, there will always be some computers that are left vulnerable — especially at a time when many information technology departments are understaffed.

Adapted from Peterson, Andrea, and Craig Timberg (2014, Oct 17) Stop worrying about master hackers. Start worrying about the IT guy. Washington Post*. Retrieved from www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/stop-worrying-about-mastermind-hackers-start-worrying-about-the-it-guy/*

Check your comprehension of the reading:

1. What was the primary cause or source of the security problem described in the text?

In short: human error. Some systems were not properly secured by the system administrator (and Oracle had weak default security settings). Oracle's Reports software had a security flaw and although they issued a patch, many systems are still vulnerable.

2. Who was affected by the security problem?

Users running Oracle's Reports software, notably universities and government agencies in the US

3. What types of data were exposed by the security flaw? Name at least three types.

- communications records, doctors' names, email addresses phone numbers in UCLA health system
- names of children & their birth dates in Texas – children who should be protected by the state for many different reasons
- logs of visitors to the port of Baltimore (military port!) including information about foreign diplomats, ID numbers of intelligence officials, State Department employees and officials from the Defense Intelligence Agency
- Social Security numbers of college students – in the USA, you can steal someone´s identity with their social security number.

4. What role did Russian and Chinese hackers have in the security problems?

None at all. They always get blamed for such actions but in this case, they were entirely innocent

5. Why weren't system administrators able to sufficiently protect the systems they are responsible for? Name at least two reasons.

- Sysadmins are only human and can make mistakes.
- IT departments are frequently understaffed and one individual is responsible for maintaining a large number of software and hardware.
- The Oracle product was delivered with weak default security settings.
- The Oracle system is complex.

6. How did Oracle respond after the security problem was discovered? Was this response effective?

The problem was discovered in 2011, and in 2012 Oracle issued a patch. This patch was effective for systems that downloaded it – but many users still (2014) have not installed the patch.