Vertix
it je naše starost

School network & students

Discussion about chosen security themes

Jan Jedlicka, Junior system specialist, Vertix

Co-funded by the
Erasmus+ Programme
of the European Union

School network & students

Protection is main word here. But who is protecting what? And how?

We shall discuss few chosen parts of network protection, focused od shool specifics.
Main parts will be:

- ✖ Content filters as basic protection tool
- ✖ Data protection, including backup and encryption
- ✖ Most common attacks again networks these days
- ✖ Monitoring and logging

Content filters

When protecting students, many schools rely heavily on content filtering. Well, protecting students… Forbidden fruit tastes best. What do you think about content filtering? Does it really protect students, and from what?

- Do you use it?
- Do you believe it is a good thing, or do you see it more like sort of censorship? Where do you think is border?
- Do you think it is reliable? How easy or hard is to get around it?
- Who should decide what to block?

Data protection

Now a bit about our data. At school, we are dealing with very, very sensitive sort of data. Do we care about them enough?

- Where and how are our data stored?
- If in cloud, do we have any guarantees from cloud provider?
- If on our servers, how is server secured? Do we backup? And how? How are backups protected?
- And, what about encryption? Do we use it? For example, on backups? And what about disk encryption, like bitlocker?
- Is our communication encrypted, for example when entering school credentials to e-learning system? Do we know how are these credentials stored?
- How do we choose who can access our data? Do we know who can do what? And do we have logs about what was done?

Most common attacks and how to deal with them

School network is not different from any other computer network. Also threats are similar, yet there are some differences. Mainly because of students – they are smart, and eager to test their abilities.

But first common threats. Let’s start with most recent – ransomware. This goes hand in hand with backups, discussed earlier.

- Have you ever sufferd from ransomware attack? How did you react?
- How do you think you could find and stop ransomware before the damage is too big?
- What do you know about mechanism of this attack? (encrypting older files first, attacking a machine that was not the original source of security breach, deleting existing backups…)

Most common attacks and how to deal with them - botnets

Another big problem could be malicious software that would turn school computers into obedient part of some bot-net. This can have serious consequences, for example when this botnet is used to attack i. e. local government website with ddos attack.

Our whole network could be infected and wasting it's resources for someone else's good. Bitcoin mining seems pretty harmless, but it is school who pays for electric energy :-) Plus, these botnets are for hire. And not for much. How do we fight this threat?

Most common attacks and how to deal with them - phishing

No infection can be prevented at 100% success rate. But we can minimize the damage if we set proper monitoring, have reliable backups at hand, and most importantly – we educate our users. We are school, after all.

Educated user is less vulnerable user. This works for every threat discussed earlier. And it also works for last of threats chosen for today, scam mails, phishing and so called fake news. This themes are very actual here in Czech Republic.

- What is phishing, do you know the term? Do you know basic signs of phishing sites
  - no https or wrong certificate, wrong domain, risky source of link, different look of the website…
- What to do when our students suffer from this attack and come to us for help? Can we provide them with relevant information and help (change passwords, notify bank, block credit cards and so on)
- And what if our own server got compromised and hosts a phishing website? Can we react to this, can we even detect it? (Disabling website, identify breach, keep logs for possible future use…)

Most common attacks and how to deal with them – ransom mails

Phishing is highly successful evolution of spam mail, but it can be easily fight with education. Smart and educated users are less likely to fall into this trap.

Nowadays, new subsort is on the rise. It comes along with the success of ransomware. Ransomware encrypts whole disk and asks for money, but there is easier way – to simply pretend that attacker has some sort of important information and will make it public if a victim refuses to pay.

These ransom emails are easy to forge and they can be sent with use of botnets on really low cost. And there is always someone who will pay. And again – there is only one weapon against it. Education and generally, not acting stupid :-)

- There are some common signs in these mails. Which are they?
    - Bitcoin transaction, poor translation even in English versions, unrealistic claims like webcam recordings when no webcam is present…
- Do we include this new phenomena when teaching ICT?

Most common attacks and how to deal with them – monitoring

Last but not least, let’s talk about monitoring and logging
Monitoring of our networks, computers and user behavior is also important part of prevention. But it is also essential when recovering from some sort of breach. It is necessity to have relevant logs to identify a problem.

We are not talking about monitoring a communication content, that would by a different story – most probably illegal. But we should have knowledge for example about the fact that some our computers have active communication with servers in suspicious areas, usually abroad (Asia for example) – that could raise an alert. Or which account is being used to something unusual, and block that account because it is probably compromised. Monitoring is vital part of proactive protection.

- Do you know for how long are logs stored at your school? Do you know what is being logged?
  - Network connections, user actions like “file created” or “settings changed”…
- Are these logs evaluated and how? Automatically with some sort of software, or manually by your IT staff?
- And because we are schools – are our students aware that literally nothing goes unnoticed, regardless of what they may have heard about internet anonymity? (And, do they know how to hide themselves better when needed, like with TOR network?)

Thank you!

Thanks for the discussion, is there anything else you would like to ask?

Vertix
it je naše starost

VERTIX s.r.o.
Štrossova 291
530 03 Pardubice

www.vertix.cz