ETH zürich

CYBER GROUP
ETH STUDENT INITIATIVE

Future Challenges

Cyber Group Meet & Greet
20.10.2021, 18:15

vseth Organisation Verband der Studierenden an der ETH

About Cyber Group

Cyber Group ETH Student Initiative is an organisation by students, for students, that aims to foster cyber-enthusiasm at ETH.
We bring academia, industry, and public institutions closer to ETH students through a variety of events. We are interdisciplinary, spanning the entire spectrum from Computer Science and Electrical Engineering to International Studies, Policy, and Military Academy students, with everything in between. But the most important thing about us is that we are all passionate about cyber security, and we want to share our passion with our fellow students!

We structure our activities around three pillars: Open Ports, the Cyber 09/12 Strategy Challenges, and the Meet & Greet.

Open Port

We have a variety of Open Port events during which renowned cybersecurity experts will come to ETH to discuss their field's current state with a small group of students. Our Open Port events are there to communicate, connect and learn from each other. And in true ETH fashion, most Open Ports are followed by an Apéro.

Cyber 09/12 Strategy Challenge

The Challenges are annual cyber policy competitions where students worldwide compete in developing national security policy recommendations to tackle a fictional cyber incident. You will be given a crisis situation that you need to solve in a team. You will need to work out a strategy to tackle the problem and then present and justify it in front of a jury. But don't worry, Cyber Group will prepare you with a thorough preparation ahead of the competition!

Meet & Greet

The Meet & Greet is our annual networking event, which allows cybersecurity enthusiasts from every field to discuss, socialise and enjoy an evening of talks. This makes the Meet & Greet a unique opportunity to learn more about cybersecurity, to listen to real stories about cyberattacks, and get in touch with many interesting people.

Scenario E: To vote or not to vote?

The Republic of Eklosia is holding an important election, which is predicted to have a very close outcome. The opposition has strong support. This is partly due to an ongoing pandemic, in response to which the government enacted measures that many disagree with.

To enable people to vote from the safety of their homes, the Eklosian government has introduced online voting. *DigiVote* is planned to be open between 8 AM and 6 PM on election day, alongside traditional physical polling stations.

DigiVote's source code was open sourced for public review. Four days before election day, a well-known academic researcher who is very active in the opposition party contacts you to responsibly disclose an issue (i.e. without yet going public). They claim that the e-voting scheme has a flaw that allows an attacker to break "vote privacy". Anyone could see who voted for whom! However, the researcher provides only a theoretical analysis and not a practical proof-of-concept.

You are advising the nonpartisan election commission.
What do you recommend?

1. Urge the government to pass an emergency law to postpone the entire election until the technical problem is solved. Online voting should be available to all citizens.

2. Cancel the online voting and call on people to vote in person instead.

3. Issue a press release addressing the report, but arguing that the attack is only theoretical with no practical implications, and that the elections will be carried out offline as well as online as planned.

4. Alert the domestic CERT to investigate the claim and delay a decision until you have more information.

Scenario T: An Endless Stream?

You live in Downtown, the bustling capital of Downstreamia. Since Downstreamia is mostly desert, you are reliant on the water from the Great River Dam located in your neighboring country Upstreamia for your agriculture and freshwater supply.

However, the two countries had tumultuous relations in the past, as both were established after a civil war that split the Streaming Republic.

One morning, a large fraction of the dam's valves don't open anymore. Water flow is significantly reduced, threatening a drought.

An Upstreamian spokesperson claims they were hit by ransomware. In addition, due to unfortunate circumstances, the manual override has failed.

You are an advisor to Downstreamia's government.
What do you recommend?

1. Work with Upstreamia's authorities to cooperatively investigate the attack that negatively impacts the countries' water and energy supplies.
2. Hack Upstreamia's SCADA system to take control of the valves.
3. Set the country into a state of emergency and prepare drought relief measures.
4. Publicly condemn Upstreamia's use of the vital water supply as a political pressure point.

Scenario H: Breaker of Supply Chains

You are the CISO of the vaccine company VCorp. Though your main production is based in Switzerland, VCorp's supply chain is distributed all across the EU.

An hour ago, you received an anonymous email. The sender claims to have hacked one of VCorp's suppliers in Eastern Europe and to have interfered with the vaccine manufacturing and quality assurance process. Along with their threat, the source sends you secret documents internal to the supplier.

You don't know at what exact point of time the attack started, and if the vaccine batches produced since the alleged attack are safe.

At the same time, VCorp is also receiving reports of health issues that may be related to the vaccine, but this has no statistically significant evidence yet.

You are now in the boardroom of VCorp.
What is your highest priority as the next step?

1. Issue a public warning and work with the government to call on people who already received the vaccine to sign up for a medical checkup.
2. Stop your current production and test the produced vaccines that haven't yet been shipped to identify potential issues.
3. Commission a forensic investigation of your ICT infrastructure to verify the claims and confirm that a cyber security attack occurred.
4. Notify law enforcement and file a report.

Thank you for participating!

Thank you for taking part in our Meet & Greet! We hope you enjoyed the opportunities to meet students and experts, and that you had fun solving our mini-challenges.

We strive to organise the very best events we can, and you can help us by filling out our short feedback survey (see below). It only takes a few minutes, and will help us organize an even better Meet & Greet next year!

If you would like to know more about what we do and how you can be part of it, please reach out to us at mail@cybergroup.ch!

Follow us on social media and sign up to our newsletter to be informed of all our upcoming events, and to follow the adventures of our Cyber 09/12 Strategy Challenge Teams!

Feedback **Newsletter** **Twitter** **LinkedIn**

Cyber Group ETH Student Initiative
c/o VSETH
Universitätstrasse 6 / CAB
CH-8092 Zürich

cybergroup.ch
CyberGroupETH
cyber-group-eth