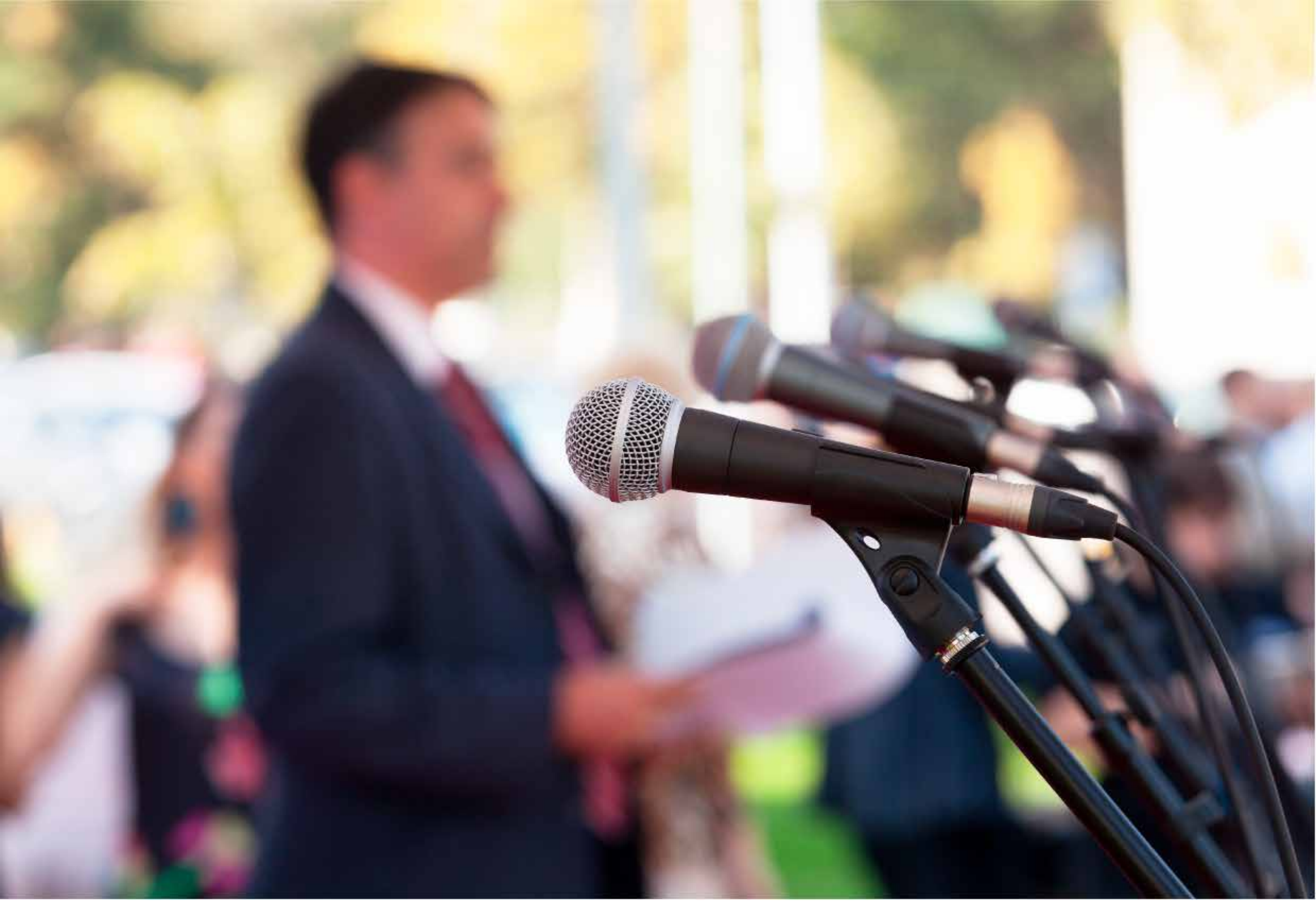

Ministry of Interior,
Republic of Serbia

2019

Cyberattacks and crisis communications: a matter of reputation

kaspersky BRING ON THE FUTURE

Kaspersky
Incident
Communications

The Ministry of the Interior is a cabinet-level Ministry in the Government of Serbia.

www.mup.gov.rs

- Located in Belgrade, Serbia
- 42,817 employees
- Uses Kaspersky Incident Communication

The Ministry is responsible for local and national law enforcement and police services with district and municipal branches throughout the country.

The Ministry's core responsibilities include crime prevention, criminal apprehension, investigations, customs and border control, counter-terrorism, anti-corruption, anti-narcotics and disaster relief. The Ministry is also responsible for issuing passports and personal identification documents to citizens.

Challenge

When cyberattacks occur in large-scale government or private organizations, the first step is to acknowledge the incident. The second is deciding how to disclose the necessary information without damaging their own reputation. In 2018, the average financial impact of a data breach was $1.23 million for enterprise level companies. This is a high price to pay, which means that mitigation requires a wide pool of people. And not all of these people, including PR and management, are necessarily familiar with cybersecurity essentials. However, in order to respond quickly and efficiently, all members of the crisis response team must know each other and know what to do.

"**Communication to the public about major cyber incident is crucial, especially for government organizations like us, because we collect and store data from citizens. Any doubt in our ability to protect private data will impact our reputation and result in people no longer trusting our Ministry and other government services. Timely and meaningful communication to the public will prevent rumors and disinformation.**" explains Nebojsa Jokic, Head of CERT , Ministry of Interior, Serbia.

"Rapid and effective communications are even more challenging for EU companies. They need to notify regulators about attacks and personal data breaches within 72 hours. That basically means the company needs to be prepared to react to incidents within just 3 days." adds Vitaly Mzokov, Head of Innovation Hub at Kaspersky.
The main challenge and risk in public communication about cyberattacks lie in exactly how to disclose the information. How to share the information that the company is required to share and yet not to risk damaging its reputation – is this the art of PR or a deep understanding of the threat? Badly communicated news about a company being hacked affects the company's public image more than the cyberattack itself.

> "During the practical exercises the PR team learned how cyber incidents are different from the other crisis situations they are used to handling. Previously, they had not even realized that a cyber incident might ever occur in the Ministry network".
>
> **Nebojsa Jokic, Head of CERT, Ministry of Interior, Republic of Serbia**

Experience is the best teacher

When you want to learn more, don't you prefer working with somebody that has firsthand experience? Kaspersky experienced an advanced persistent threat (APT) named Duqu 2.0 back in 2015 and managed both the security breach and the necessary communications outstandingly.

EXPERIENCE
Kaspersky builds training materials based on a real-life targeted attack they underwent, mitigated and made public successfully

EXPERTISE
World famous security experts working with top PR professionals create operative synergy

WORKSHOP
A workshop tailored for each organization results in an **Incident Communication Plan** designed for the given organization

At the end of the day, the public announcement about Kaspersky being attacked didn't damage company's reputation and impact customer relationships. In fact, both customers and the market now trust Kaspersky even more than ever.

"We decided to have the **Kaspersky Incident Communication** training for key personnel from IT Security, PR and CERT teams: 7 key people in total, who would be managing a cybersecurity incident. If it happened to Kaspersky, it could happen to anyone," shares Nebojsa Jokic.

"When we at Kaspersky realized that our infrastructure is under targeted attack, in addition to the IT team and cybersecurity experts working on mitigating the attack, we had a PR team prepare statements for global and regional media because the company management was 100% sure that the incident needed to be disclosed.", Vitaly Mzokov relates, "It took us 3 months to sort things out and throughout those months the process was managed in top secret mode, since we wanted to act before the attackers realized that we are aware of them. This was the key to success. We kept all communication encrypted and used several other techniques to maintain the strictest confidentiality."

Our success inspired us to wrap up our experience and tips into the **Kaspersky Incident Communication** training and offer it to organizations that want to be prepared for such incidents. Because it is too late to start planning when you are under attack. A single email can disclose your actions to the cybercriminals. Then they will be able to strike first and no one knows how it will impact your company's reputation."

"**Kaspersky is famous for their Endpoint solution, but also for a great Enterprise portfolio, as well as expert positioning in the global market. When we had an opportunity to organize a training with Kaspersky experts, we seized the opportunity,**" continues Nebojsa Jokic.

It was a great idea to bring people with such different roles who had never met each other within a large organization such as our Ministry to the same table and challenge them with a targeted attack training session. We all learned what is best to do in case of an attack: what and how to communicate to the public, which tools to use, what media and journalists to involve. It turned out that there is a right way to do it, which leads to success, but this works only if regular collaboration and open communications occur between technical and PR teams."

4 sec

Time needed by hackers to infect a single laptop with a simple USB stick

72 hours

Time specified by GDPR for organizations to notify regulators about data breaches

3 months

Time it took Kaspersky, a cybersecurity expert, to properly prepare for disclosing a cyberattack

The training includes all aspects of communication, internal and external. Not just what information to share with the public and how, but also how to send internal messages to colleagues, what equipment to use, and how to hide this activity from the attackers.

The hands-on workshop is the key element of the training: the workshop is prepared in advance and is based on specific customer needs. The participants are given real world simulations to manage.

Practice makes perfect

The goal of the **Kaspersky Incident Communication** training is preparation for the worst scenario: the workshop section enables the participants to produce their own **Cybersecurity Incident Communication Plan**.

"One particularly useful result of the training was the realization that we need to work on increasing awareness about cybersecurity inside the organization among the senior management. They, too, have to realize that the danger is significant, and measures need to be in place now, as the aftermath could be very serious," continues Nebojsa Jokic. "During the practical exercises the PR team learned how cyber incidents are different from the other crisis situations they are used to handling. Previously, they had not even realized that a cyber incident might ever occur in the Ministry network.

The presentations described the cyberattack from inside. The Kaspersky team shared how the company countered Duqu, a sophisticated targeted attack, and our staff appreciated the practical nature of the session."

"I believe that Kaspersky is one of the greatest companies in the field of cybersecurity and their experience in counteracting targeted attacks makes their Kaspersky Incident Communication training truly useful and practical." – concludes Nebojsa Jokic, Head of CERT, Ministry of Interior, Republic of Serbia

Website: https://kas.pr/kic
Email: kic@kaspersky.com
Cyber Threats News: www.securelist.com

www.kaspersky.com