Ukraine Crisis for Telecom: Increased Preparedness and Lessons Learned

ENISA Telecom Security Forum

KPN CISO | June 29, 2022

kpn. Het netwerk van Nederland

Introduction

This presentation elaborates KPN's response to the Ukraine crisis, which focuses on:

1. Creation of situational awareness of emerging threats;
2. Preparation for possible cyber incidents;
3. Lessons learned.

Observations and actions from the first days

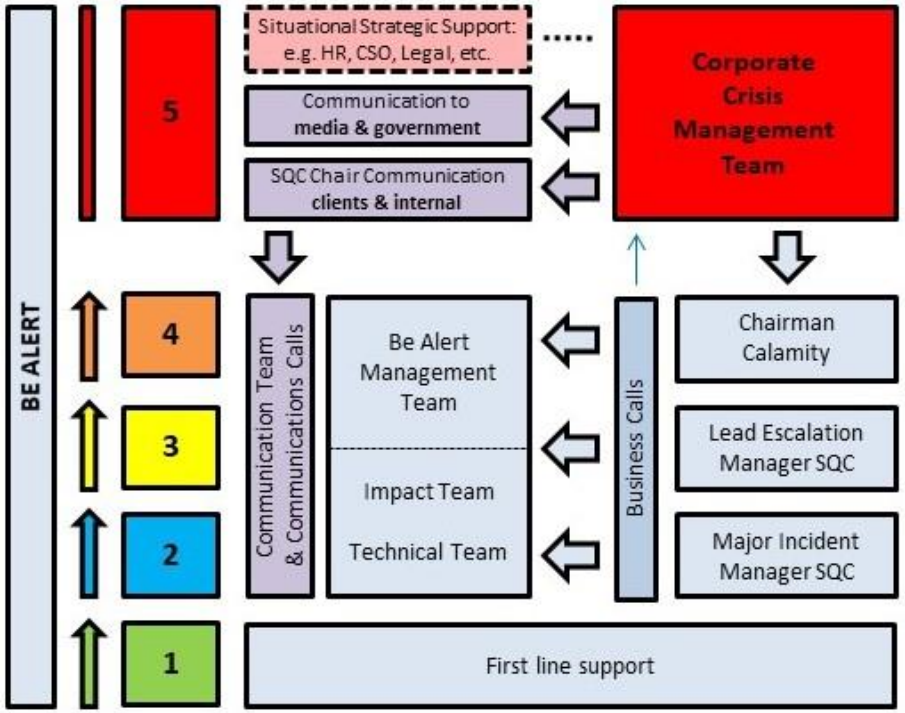
Outside-in: External Developments; Emerging Threats

- Continuous DDoS attacks (CERT-UA warning)
- Disruption of Satellite Internet Connections (Viasat)
- Wiperware (e.g., WhisperGate and HermeticWiper) and other malware attacks

Inside-in: Internal Actions; Increase Preparedness

- Start a precautionary “Confidential Be Alert” (daily report out to the Board of Management)
- Contact government, relevant authorities and other partners
- Suspend broadcasting of 5 Russian outlets (based on EU directive)

KPN initiated the major incident management process to be ready to respond to any cyber incident.



To prepare for possible escalation of the crisis in Ukraine, including any potential security events as a result, KPN has initiated its major incident management procedures. As a precautionary measure, KPN has started a “Yellow Be Alert” to monitor the situation with all relevant internal KPN stakeholders, inform the Board of Management and external and governmental stakeholders and be ready to respond when required. A Yellow Be Alert is the second step in the major incident management process, putting KPN on “high alert”. It involves amongst others daily meetings with KPN’s security analysts, business representatives and corporate advisors.

KPN has currently scaled down to “green”.

KPN intensified information gathering en re-evaluated the effectiveness of security controls.

Information sharing and collaboration with government and other partners intensified:

- Building on existing and strong partnerships
- New relationships established, e.g., with Financial Services ISAC

The effectiveness of the cybersecurity framework has been re-evaluated:

- Updated the Threat Assessment
- Implemented Safelinks/Safedocs
- Reviewed and extended coverage of the SOC
- Conducted Purple Teaming exercise
- Verified Back-up & Restore capabiliti

KPN has reviewed the implementation and monitoring of baseline & risk-based security measures.

Regulatory Measures in NL to improve Security and Integrity

	Baseline Security Measures (examples)	Additional Risk-Based Measures (examples)
Identify	Espionage Threat Assessment Cyber Threat Intelligence	Extended Threat Assessment (Disruption, Sabotage)
Protect	Identity & Access Management Encryption	
Detect	Continuous Vulnerability Management Security Monitoring Penetration Testing	Red & Purple Teaming Exercises Threat Hunting
Response	Incident Response (CSIRT), and Major Incident Management (Be Alert)	
Recovery	Business Continuity Management, including Technical Recovery Testing	

5G Security Controls Matrix

Lessons learned and conclusions

Observations and lessons learned:

- Collaboration with authorities is good, but more information sharing is still needed.
- More coordination is welcome but avoid duplications.
- Threat assessment should focus on espionage, disruption and sabotage.
- (Re-)evaluation of security processes, procedures and tools result in unexpected findings.

Conclusions and recommendations:

- Set up a Security Be Alert process at a European level.
- ENISA's 5G Security Control Matrix provides a good foundation for implementation and monitoring.