IstroSec

Data Sheet

Incident Preparedness Assessment

The probability of cybersecurity incident and the following consequences is increased constantly. It is possible to lessen this risk by implementing appropriate preventive, detective, and reactive precautions. But how will you know which technical, organizational, or procedural measures you need to take? Experts from **Istro**Sec have years of experience with resolving cybersecurity incidents in organizations from multiple fields. We are ready to help you with assessing the preparedness of your organization and how effective would you be in dealing with cybersecurity incidents.

In the scope of your assessment, we focus on:

Human resources

- Responsibility for dealing with cybersecurity incidents
- Size, aptitude, and preparedness of your team for resolving cybersecurity incidents
- 3rd parties and their role in resolving incidents

Processes

- Incident prevention
- Incident identification
- Initial incident analysis
- Containment, Eradication and Recovery
- Digital evidence and forensic analysis
- Continual improvement

Technology

- Infrastructure and network architecture
- Setting of network components - switches and routers
- Setting of security components - firewalls, UTM, IPS/IDS, NBA, application firewall
- Setting of security oversight, systems for detecting and reacting to incidents
- Setting of servers - Windows, Linux, Unix
- Workstation setting
- Setting of domain policies and GPO
- Cloud system settings - O365, Azure, AWS
- Critical application setting
- Backup settings

Material and documentation

- Asset inventory
- Incident documentation
- Threat intelligence
- Network topology
- Security policies and regulations
- Procedures for resolving incidents
- Escalation procedures
- Contacts and contact schemes

Why IstroSec?

Combined experience of more than 70 years

Access to experts in all domains of information security, including penetration testers, forensic analysts, malware analysts, trainers and more

Systematic improvement of information security according to frameworks enriched with the experience of IstroSec experts with advanced security incidents

Certified experts to ensure compliance with security standards and legislation - **Istro**Sec experts have been operating in public administration (NIS Directive, GDPR and others) as well as in the private sector (ISO 27001, NIST, HIPAA and others)

IstroSec

Data Sheet

Our Methodology

Our assessments for cybersecurity incidents are based on best practices and years of experience with resolving cybersecurity incidents, knowledge of current vulnerabilities, techniques, tactics and procedures used by the attackers during cyber-attacks.

To be able to assess your organization's cybersecurity incident preparedness most efficiently, our team at IstroSec developed a unique methodology. Through this methodology, we achieve coverage of relevant security needs of our customer. Furthermore, we focus on implementing a set of procedures with biggest impact on the ability to deal with cybersecurity attacks, while minimizing time to resolve, the technical and financial cost.

Our methodology is based on these pillars:

Threat Landscape

- Creation of "Threat landscape" for organization, in which experts at IstroSec analyze relevant threats for your organization based on threat intelligence, type, size and sector of organization. Including potential previous breaches, OSINT (clear and darkweb), geopolitical situation, specific organization and threat score calculated based on technologies you employ.

TTPs

- Identification of tactics, techniques, and procedures (TTPs) used by attackers
- Assessing procedures, technologies, and capacities relevant to identified threats

Documentation, Interviews, and Config

- Inspecting relevant documentation
- Assessing preparedness in the form of interview with employees
- Assessing preparedness by inspecting configuration of implemented technologies

Assess to Improve

- Vulnerability assessment
- Analysis of current state and suggestions for improvement

Report

- Preparedness assessment, creation of final report and recommendations

Implementation & Exercising

- (Optional) Implementation of proposed procedures and relevant processes
- (Optional) Conducting technical exercise in order to verify effectiveness of implemented procedures on technical and procedural level by:
  - Tabletop exercises

IstroSec

Data Sheet

Why Us?

Experience and knowledge

IstroSec experts have long-standing experience with improving cyber-attack resiliency for organizations of various sizes and from different sectors. They maintain current knowledge about cyber threats, tactics, techniques and procedures used by attackers. Combining this knowledge with plentiful experience in actual incident response allows our specialists to create a tailored set of administrative and technical measures for your organization to create a resilient and robust cyber immunity.

Expertise in incident response

IstroSec specialists have expertise in assessing the preparedness of our client to face cyber-attacks and related areas, such as digital forensics analysis, and world-class malware analysis, which they have repeatedly demonstrated while dealing with state-sponsored cyber-attacks, attacks on Fortune 500 organizations, as well as the participation of four **Istro**Sec experts in the winning team of Locked Shields 2016 exercise.

Certified professionals

IstroSec experts are also holders of internationally recognized certificates in these areas. We hold certificates such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) and more.

Case Study

Company type: Big fintech company

Service provided: Incident preparedness assessment

Solution: Assessment of IR maturity and attack simulation

Big Fintech organization approached us with request to assess their maturity level of their capabilities to respond to incidents relevant to this organization. Organization was already ISO 27001 certified and held their PCI DSS certifications.

IstroSec systematically analyzed the threat profile of the organization and determined that aside from standard threats against organizations like ransomware and similar, this organization could be also targeted by more sophisticated attacks because of their position on the market, the number of institutions and organizations which used their software and their financial results. There was compiled the list of attacker tradecraft and TTPs to create baseline against which the assessment was being conducted.

IstroSec utilized its methodology to assess documentation, processes, and technology. Organization had implemented ISO 27001 and systematically follows all procedures required. Also, they had competent security team which followed the procedures to the letter. However, during the assessment it was discovered that the security of the organization is focusing on compliance with regulations and standards but there were key components missing to be capable of responding to the actual incidents.

IstroSec proposed 283 configuration changes in active directory, cloud environments, endpoints, network and security solutions, log management and SIEM. Each of these was targeted to detect, disrupt, deny, degrade, or deceive attacker`s specific TTP used which was relevant to the organization. It was also discovered that the organization does not have effective processes regarding containing security incidents and some of the gaps in escalation of incidents to facilitate proper reaction were also found. Furthermore, changes to processes were recommended and the implementation of these changes was supported.

After implementation of recommendations the attack simulation was conducted to test the effectivity of implemented controls.

IstroSec | Černyševského 10 | 851 01 Bratislava | Slovakia | +421 917 699 002 | info@istrosec.com | www.istrosec.com