PRONTOCYBER®
BY CY4GATE

Digital Emergency Response for Cyber Security Incidents

White Paper

White Paper

CY4GATE

Rev. No. 1 of 08/08/2022

PRONTOCYBER®
BY CY4GATE

Summary

PRONTOCYBER®
BY CY4GATE

1 Digital Emergency Response

1.1 Cyber Consultancy

An Emergency Cyber Response allows clients to receive immediate support in the event of a cyber-security breach.

The service is provided by resources with specific skills and know-how in the field of Security Incident Management and with Incident Response experience, even concerning complex situations.

To support and guarantee the correct and prompt response in the event of incidents and/or hostile attacks, a process compliant with the ISO/IEC 27035 standard is adopted, consolidated and enriched by many years of experience in CERT environments.

When required, an Emergency Cyber Response also offers support and possibly coordinates the activities necessary to restore the proper functioning of the services impacted by the incident.

Ready for Cyber Response – Objectives:

- To quickly detect any violation and identify the most appropriate response strategies;
- To significantly minimise response times and damage caused;
- To gather all information necessary to support any eventual legal action;
- To shield the client's reputation and assets;
- To assess the implications of best practices of sector and current regulations (Privacy, etc.);
- To analyse the incident that occurred by identifying errors, weaknesses and strategies adopted for management, improving the response to future incidents.

Emergency Cyber Response – Incidents Managed:

- **PERSISTENCE**
- **INCREASED PRIVILEGES**
- **DEFENSE EVASION**
- **ACCESS TO CREDENTIALS**
- **DISCOVERY**
- **LATERAL MOVEMENT**
- **EXECUTION**
- **COLLECTION**
- **EXFILTRATION**
- **COMMAND & CONTROL**
- **DENIAL OF SERVICE (DOS)**

1.2 Legal Consultancy

Legal Intervention allows clients to receive immediate legal support in the event of a security breach.

The service is provided by experienced resources with specific skills and know-how in the field of legal management of security incidents.

This service will be activated following a security breach falling into the following categories:

- A confidentiality breach, meaning an unauthorised or accidental disclosure of or access to personal data;
- An availability breach, upon a loss, inaccessibility or destruction – either accidental or unauthorised – of personal data;
- An information integrity breach, so when an unauthorised or accidental alteration of personal data occurs – this particular type of breach also covers instances of temporary unavailability.

Within 36 hours from first contact, legal experts shall assess the extent of any suspected data breach in terms of its impact on personal data and the rights and freedoms of data subjects, determining whether or not there has been an actual personal data breach.

PRONTOCYBER®
BY CY4GATE

2 Cyber Assessment

Proper security management is primarily based on an adequate knowledge of the current level of protection of one's own systems.

With this in mind, a security and audit programme must include the combined activity of Vulnerability Assessment (VA) and Penetration Testing (PT), which help to understand the real security level of one's business processes.

2.1 Vulnerability Assessment

The Vulnerability Assessment (VA) provides a list of the most immediately-identifiable vulnerabilities then mitigating them by prioritising and structuring corrective actions.

Indeed, the VA activity aims to carry out a dynamic assessment of the security level of devices connected to the internal or external network and of web services and applications exposed to the outside world, in order to identify any vulnerabilities related to potential security misconfigurations, a lack of active protection levels, outdated software, unauthorised devices within the network and so on, which could expose the corporate information system to breach risks.

The VA's main objective is to verify the security and efficiency standards of the assets identified, to detect any critical issues and propose consequent corrective measures to ensure the implementation of the best security and reliability features of the system in use.

Vulnerability Assessments are thus a true analysis of all corporate IT assets, necessary in identifying and classifying risks and vulnerabilities. Mapping the entire IT infrastructure renders it possible to highlight potential critical issues to then implement the necessary prevention and protection measures for the IT system.

2.2 Penetration Testing

The Cyber Assessment service involves a dynamic verification of the security of the client's systems in order to identify any vulnerabilities, incorrect security configurations or deficiencies in the active protection levels that expose the context to external attacks. The methodology adopted refers to the international standard for executing security tests developed by ISECOM and the guidelines for application assessment activities defined by OWASP.

Based on experience accumulated, the ISECOM principles have been grouped and reorganised in line with a proven process that also includes some innovative concepts on both the classification of vulnerabilities and the representation of problems and areas of intervention, as will be described in the following sections.

As such, the purpose of a Security Assessment is to collect the information that may give rise to the interruption of a service or intrusion into the client's systems, working with a methodology borrowed from that commonly used by hackers through specific tests (intrusive and non-intrusive).

The service involves a multi-phase analysis and identification of security vulnerabilities, availing not only of an operational logic based on the use of automated tools but also of verification and attack operations streamlined by members of a highly-specialised team with specific expertise.

The team adopted a customised methodology based on a sub-set of tests designed on portions of the OSSTMM (Open Source Security Testing Methodology Manual) methodology, supplemented with a business-oriented validation process to ensure the execution of an appropriate assessment of each critical factor and modulating the method in relation to the specific technology under consideration and the explicit needs of the client.

PRONTOCYBER®
BY CY4GATE

3 Cyber Awareness

3.1 Cyber Education

The objective of Cyber Security Awareness Training is to raise participants' knowledge of cybersecurity risks, with a specific focus on different security domains.

The Cyber Security Awareness Training programme, provided in Italian, takes the form of a 3-hour and 45-minute "Learning Path" and will cover the main attacks affecting businesses, recognising the risks of surfing the internet and best practices for navigating the web safely.

Following are some training strategies that will be adopted for in order to access the Learning Paths/Webinars:

- Webinars with unlimited access;
- Verification of the participants' entry level through an entry questionnaire conducted by means of closed-ended questions in self-assessment mode;
- A combination of the frontal approach for communicating the content of the training intervention and interactive mode;
- Engagement of webinar participants using multimedia content (videos, images, glossaries, industry articles) on examples from real-life cases of cyber-attacks in business contexts;
- Verification of learning through the provision of closed-ended questions at the end of the webinar;
- Issuance of a certificate upon completion of the course;
- Time dedicated during the Webinar to questions regarding the topics covered during the course.

The training platform will be provided by the client and all necessary support will be given for integrating Webinar recordings on the existing corporate training platform.

3.2 Phishing Campaigns

Considering that the greatest security threats for organisations lurk in the email inboxes of employees and consultants, the Phishing Attack Simulation Service sees the execution of real scenarios to test and sensitise company users.

Phishing Attack Simulations are customised on the basis of the specific characteristics of the target organisation and test the team's know-how and experience in terms of red team, blue team, social engineering and state-of-the-art cyber-attack techniques and tactics.

At the end of each attack campaign, a report is produced with detailed information purely oriented towards the result, useful both in terms of risk measurement and risk reduction.

This service perfectly complements awareness training programmes, with the ultimate objective being to increase the responsiveness of the individual, who is increasingly exposed to and victimised by these types of attacks.

Phishing Campaign Phases:

- **Phase 1 – Phishing Campaign Proposal**
- **Step 2 – Acceptance and Identification of the Target**
- **Step 3 – Executing the Phishing Campaign**
- **Step 4 – Reporting**

www.prontocyber.com