hardsecure
WE MAKE SECURITY

H-CYBER E-MAIL

(E-MAIL SECURITY ANALYSIS SERVICE)

CYBER EFFECT - LEVEL 0 - UNPREPARED

This datasheet presents our service in a generic way. The actual scope and conditions of the service will have to be reflected in a technical and commercial proposal.

h·cyber E-MAIL

SERVICE DESCRIPTION

E-mail is the most widely used information exchange service in the ICT world. Financial crime is on the rise, through the fraudulent exploitation of business communication via E-mail. To this end, the attackers, often criminal organizations, use advanced resources aimed at misleading the target as to the true identity of their interlocutor and the legitimacy of the action to be carried out/authorized.

This type of crime, often framed in situations of Business E-mail Compromise (BEC) or E-mail Account Compromise (EAC), in which the attackers manage, through fraudulent processes, to make undue payments/bank transfers happen for their benefit, representing a real and quantitative risk for organizations and their value chain. In addition to the financial component, this service is used by attackers to carry out other attacks, such as data leakage, exploitation of different types of malwares to compromise the service, user equipment or in more complex cases (such as ransomware) the entire IT infrastructure.

It is increasingly important to ensure that the E-mail service is correctly configured from a security point of view and that users are made aware of the precautions to take when using E-mail.

VALUE PROPOSITION

This service aims to assess the configuration status of E-mail security mechanisms and to raise awareness among users on how to use E-mail in an informed way.

As a result of the analysis of the E-mail service configuration, a report is produced with the evaluation of the configured mechanisms and possible recommendations for improvement, which may range from the recommendation of the configuration of security protocols (such as SPF, DKIM, and DMARC), to the suggestion of licensing additional/complementary defense technologies, to address specific security gaps in the organization.

The awareness action will be carried out in a Webinar model, presenting the most common techniques used in E-mail fraud and the precautions to take for safer use of the service in a business environment.

Addressing both human and technological aspects simultaneously, this service aims to strengthen the organization's defenses against growing threats such as financial crime (E-mail fraud).

Rua Acácio de Paiva 16
1ºDto - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

hardsecure
WE MAKE SECURITY

H-CYBER E-MAIL

(E-MAIL SECURITY ANALYSIS SERVICE)

CYBER EFFECT - LEVEL 0 - UNPREPARED

This datasheet presents our service in a generic way. The actual scope and conditions of the service will have to be reflected in a technical and commercial proposal.

SERVICE FEATURES

This service is defined by the following elements:

- **Analysis of filtering and security.** Security configurations are audited to analyze them for:
  - Analyzing the IP reputation in real-time;
  - Analyzing the possibility of performing Phishing, Fraud and Spoofing attacks;
  - Verification and evaluation of DHA (Directory Harvest Attack) attacks;
  - Analyze the DKIM/Sender ID/SPF and DMARC protocols;
  - Subject, Body, and Header analysis, as well as Heuristic, Mime, and Regular Expression analysis.

- **Analysis of the security configurations and controls of the E-mail service:**
  - Data Leakage, encryption verification, IP reputation, interaction with Global Threat Intelligence;
  - Multitenant Quota Management;
  - Management of White and Blacklists and Detection of Malicious Attachments;
  - Analysis of the ability to block spam and similar vectors;
  - Analysis of storage and BCC plugins;
  - Analysis of the AD integration process with AAA insertion;
  - Analysis of the management of user access cases (permissions and accesses to security/distribution lists) to certain E-mail services;
  - Analysis of LDAP configuration to make a user directory securely accessible by configuring secure connections to directory servers;
  - Web/SOA services analysis, E-mail servers configuration (E-mail service and respective internal/external hops), Syslog-based log integration analysis, E-mail spooling, and E-mail services traffic management;
  - Analysis of remote accesses to the E-mail service based on third party technology, from devices such as smartphones, laptops, or workstations, which require access outside the limits of the organization's corporate intranet;
  - Auditing of mailbox security logs, E-mail filtering policies s/antispam, anti-malware, OAuth installed and configured and management of E-mail service management and security technology, as well as tracking of actions on various assets where the service is executed/processed.

Rua Acácio de Paiva 16
1ºDto - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER E-MAIL

(E-MAIL SECURITY ANALYSIS SERVICE)

CYBER EFFECT - LEVEL 0 - UNPREPARED

This datasheet presents our service in a generic way. The actual scope and conditions of the service will have to be reflected in a technical and commercial proposal.

- **Awareness raising action for E-mail users in the organization**
  Awareness-raising sessions for the organization's employees, in Webinar format, where some of the most common threats will be identified, as well as the most used techniques and aspects they should be aware of to try to avoid falling victim to a fraudulent scheme.

ADDED VALUE OF OUR SERVICE

Given the dependence of organizations on E-mail to conduct business, the use of various means to access E-mail, and the potential geographical dispersion of employees, the combination of the technological factor with the behavioral factor is essential for the attack surface to be reduced as much as possible and for organizations to be aware of and protect themselves against a growing threat to their business and their credibility in the value chain.

This service aims to help organizations strengthen their defenses against the growing threat of E-mail fraud by integrating human and technological aspects.

SERVICE QUOTE REQUEST

For further information, please contact us using one of the following means:

"Hardsecure – E-mail Security Analysis Service" form (available on the service page on the website)

Contact Hardsecure Account Management:
(+351) 218 278 126 (PT)
(+44) 204 538 6686 (UK)
(+1) 202 2318 9859 (USA)
geral@hardsecure.com

Website:
https://en.hardsecure.com (**"Request Proposal"** form).