EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

IT security at EMA - update on additional measures in place

Industry Standing Group (ISG) meeting, 22 November 2022

Presented by Dr Ivo Claassen, Deputy Executive Director

An agency of the European Union

Cyberattack - Context

- The incursion was identified 1 December 2020.
- Immediate action was taken to halt the attack on EMA systems at that point.
- EMA undertook a full investigation in co-operation with CERT-EU, the Dutch police, and Europol.
- EMA **checked its systems extensively** and identified all documents unlawfully accessed.
- Some of the unlawfully accessed documents including email correspondence have been made available through the ***Dark Web**** and were subsequently published by public media outlets.
- Affected companies and persons have been informed.
- EMA continued informing its stakeholders publicly through several public statements.

- (Cyberattack on EMA – update 1, Cyberattack on EMA – update 2, Cyberattack on EMA – update 3, Cyberattack on EMA – update 4, Cyberattack on EMA – update 5, Cyberattack on EMA – update 6)

* The **Dark Web** it's a hidden collective of internet sites used for highly illegal activities

Cyberattack - update

- The Dutch Police investigation has not been formally close.
- The Agency is still cooperating with the Dutch Police for its ongoing criminal investigation.
- The Agency is not aware/being informed of more documents made available on the “Dark web”.

Security enhancement taken by EMA 1/2

Since the incident the Agency has been continuously improving its cybersecurity posture aimed at strengthening its systems and processes, and at mitigating business risks with the implementation of administrative and technical controls to further protect the data managed by the Agency (e.g. CCI, Confidential, Personal data).

Administrative/Governance Actions

- The information security Steering Committee was established, to provide an Agency-wide oversight, ownership and direction to the information security strategy and its implementation plan.
- A revised EMA's Information Security Strategy and related implementation plan has been adopted.
- A security awareness and training program for Agency's staff and contractors has been developed which aims to foster a strong security culture to ensure that security is built into all operational aspects of EMA and user behaviour, increasing the overall security of the Agency.

Security enhancement taken by EMA 2/2

Operational/Technical Level

- Access Management enhanced to further support the “least Privilege” principle.
- Further enhancement of the Agency preventative process and protection, post-breach detection, automated investigation, and response.
- Further enhancement of the security information and event management capabilities with the adoption of the Azure Sentinel (Cloud-based solution) to increase existing capabilities to timely detect and respond to unknown threats and anomalous behaviour of (*compromised)* users and insider threats.
- Security Operation Center (SOC) service has been established to continuously monitor and improve the Agency’s security posture while preventing, detecting, analysing and responding to cybersecurity incidents. This new security service will perform round-the-clock monitoring (24/7, 365 days) of the Agency infrastructure.

Any questions?

Further information

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Telephone +31 (0)88 781 6000
Send us a question Go to www.ema.europa.eu/contact

Follow us on **@EMA_News**