GEIGER: Solution for small businesses to protect themselves against cyber-threats

José Javier de Vicente Mohino
Atos, Spain
jj.devicente.external@atos.net

Wissam Mallouli
Montimage, France
wissam.mallouli@montimage.com

José Francisco Ruiz
Atos, Spain
josefrancisco.ruiz@atos.net

Max van Haastrecht
University of Utrecht, Netherlands
m.a.n.vanhaastrecht@uu.nl

ABSTRACT

In a world where cybersecurity has an increasing importance, any company, regardless of what sector, size or activity is related to, should rely on tools and solutions that can help it to be secure in the best possible way. The GEIGER platform described in this paper acts as a perfect fit for micro and small enterprises (MSEs). These companies need to be protected against threats but sometimes do not have the resources (money, personnel, time. . .) to deal with them. Often, private cybersecurity solutions are either expensive or hard to implement for micro and small companies. However, GEIGER is designed to bring cybersecurity principles, security countermeasures and awareness in a smooth and friendly way, with special focus on the MSEs. Its ability to adapt to new challenges comes in handy when dealing with sophisticated threats and the functionalities provided to help MSEs adopting a more prominent security posture. Having the support of an innovative solution can help MSEs to achieve a more effective approach regarding cybersecurity, which leads to a better overall business management and operation.

CCS CONCEPTS

• **Cybersecurity**; • **SME and MEs**; • **Risk indicator**; • **Information Sharing**; • **Training**;

ACM Reference Format:
José Javier de Vicente Mohino, Wissam Mallouli, José Francisco Ruiz, and Max van Haastrecht. 2021. GEIGER: Solution for small businesses to protect themselves against cyber-threats. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3465481.3469202

1 INTRODUCTION

Micro and small enterprises (MSE) are increasingly "going digital". This also increases the likelihood of incidents due to negligence or malicious attacks. It is crucial that these small businesses are aware of their risks related to data protection, privacy, and cybersecurity, and get help in reducing them. There are plenty of solutions available, but they do not match the needs of small businesses with no expertise in digital technologies or resources to invest in costly and complicated solutions.

Each MSE has limited knowledge of its own security, privacy and data protection vulnerabilities, and awareness of the risks of similar MSEs or the whole community is low. This lack of knowledge implies an inability of the MSEs to understand its safety in relation to cyber threats, i.e., whether there is any need for action, and what it should do to avoid or mitigate risks[1]. While many MSEs have been convinced in the past that they are too insignificant for an attack, this perception has been proven wrong. In fact, most of the MSEs businesses have already been victims of cyber-attacks. MSEs are not only targets themselves, but often entry points for attacks on larger organizations about customer or supplier relationships. Thus, cyber-attacks and the associated damage can reach a strategic scale and affect the entire economy[2]. For this reason, every MSE in Europe must increase their efforts to protect themselves against cyber-attacks. It also must need help, e.g., through their professional associations, to make this extra effort, and finally it needs to be monitored, because of the strategic relevance and the potential exponential impact of a single attacked (networked) MSE.

To reach MSEs with security and data privacy topics, for them to become part of the EU-wide security and data protection community and be recognized as relevant, serious partner, e.g. for data sharing with CERTS/CSIRTS, we conceived GEIGER framework in the context of H2020 GEIGER project[3].

In this paper, we present an overview of GEIGER objectives (Section 2) and its main architecture and components (Section 3) and discuss its innovation (Section 4). The solution is being implemented[4] and a first prototype will be validated as future work (Section 5).

2 GEIGER PLATFORM

2.1 What is GEIGER?

GEIGER is designed as a comprehensive cybersecurity platform for MSEs. It covers various aspects including protection, awareness,

ARES 2021, August 17–20, 2021, Vienna, Austria
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3469202

[1] CyberFort. (2019). Cyber Risk: A new world for Business Continuity? www.theagenci.com/app/uploads/2019/05/Agenci-Cyber-Risk-A-new-world-for-Business-Continuity-whitepaper.pdf

[2] Director's Handbook on Cyber-Risk Oversight, 2020

[3] https://project.cyber-geiger.eu/

[4] A demonstration of this framework can be presented during the workshop.

and training for users, and it has been designed to be integrated smoothly without disturbing the company's activities.

The possibilities of GEIGER are diverse, including availability on different platforms, the support of updated information provided by cybersecurity entities such as the CERTs, the integration with other cybersecurity tools, and a sophisticated risk level algorithm.

2.2 GEIGER objectives

GEIGER has various objectives, including the following:

- Raise cybersecurity awareness on users of the platform. This remedies lack of consciousness users may have regarding the risks and threats they face every day.
- Manage and deal with the privacy of the MSEs, something which entails big importance nowadays when information is handled by third parties.
- Deliver cybersecurity training for the users at the various levels that may be required. This also includes solving cybersecurity questions.
- Contribute to achieving a higher level of protection for the MSE. The GEIGER Indicator provides information conveniently updated which leads to more consciousness for the end-users.
- Accomplish a smooth integration and deployment with no significant disruption to the business' activities.
- Provide updated status of the risk level of the business as well as other cybersecurity risks, threats, and vulnerabilities. This is achieved through frequent updates provided by cybersecurity specialists, including CERTs.

3 OVERVIEW OF GEIGER ARCHITECTURE

GEIGER has been designed according to the following architecture:

Amongst the very different GEIGER features, one of the most important refers to availability: GEIGER can be accessed no matter if the end-user is connected on a laptop or mobile and regardless of the moment. Thanks to the cloud features, GEIGER delivers on a 24x7 basis. However, although the internet is fully integrated into our daily lives, there may exist several occasions where connectivity may be an issue. This scenario, labelled as non-internet or offline, has also been envisaged in the design of GEIGER. According to these premises, the GEIGER architecture has been designed including the components described in the following sections.

3.1 GEIGER cloud

On the one hand, GEIGER relies upon a cloud infrastructure to provide continuous information and protection. GEIGER normal operation also includes interaction and integration of a variety of tools, both deployed in the GEIGER servers (i.e., internal or also known as "GEIGER Infrastructure tools") and external to the platform (or "GEIGER External tools"). The GEIGER Cloud is an intermediary or point of contact to all those tools, which enhance GEIGER capabilities by means of providing different competencies such as detection of intruders, assessment of risk, or fraud detection. Any external tool will have its sensors deployed into the device in such a way that they can provide data to their private server and, from this to the GEIGER platform.

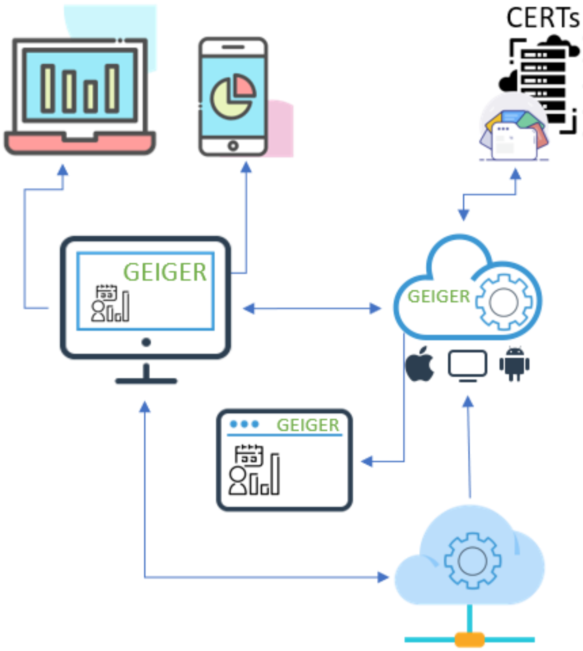

Figure 2: GEIGER global architecture

Regarding data flow, information is meant to be easily exchanged with external entities such as the mentioned tools or even security-oriented organizations such as the CERTs. These security specialized organizations are required to feed the platform with updated information of the most recent threats, attacks, and vulnerabilities, which must be used when performing the risk level calculations.

Besides, online knowledge storage is needed to centralize all data gathered. For that purpose, GEIGER comes with a cloud database that includes the correspondent API for data retrieval. This API is the GEIGER Cloud Adapter.

Finally, data exchange is key for GEIGER and, especially, for the GEIGER Cloud. To assist in the process of sharing, GEIGER has the Information Sharing Platform, the component responsible for orchestrating data delivery and filtering amongst GEIGER Cloud components in a transparent way for the end-user. The JSON format has been chosen, given that it is a standard suitable for the exchange of data effortlessly.

3.2 GEIGER Toolbox

On the other hand, it must be outlined that GEIGER has a local infrastructure where, amongst other activities, risk calculation is performed. This is called the GEIGER Toolbox.

The most important sub-component for the GEIGER Toolbox is the GEIGER Toolbox Core, where local storage is located. This approach is similar to the GEIGER Cloud, given that the GEIGER Toolbox makes use of its own database, where data is gathered for the calculation of the level of risk. Local storage is periodically updated with information provided by the GEIGER Cloud. It also comes with an API known as the "GEIGER Controller" to ease

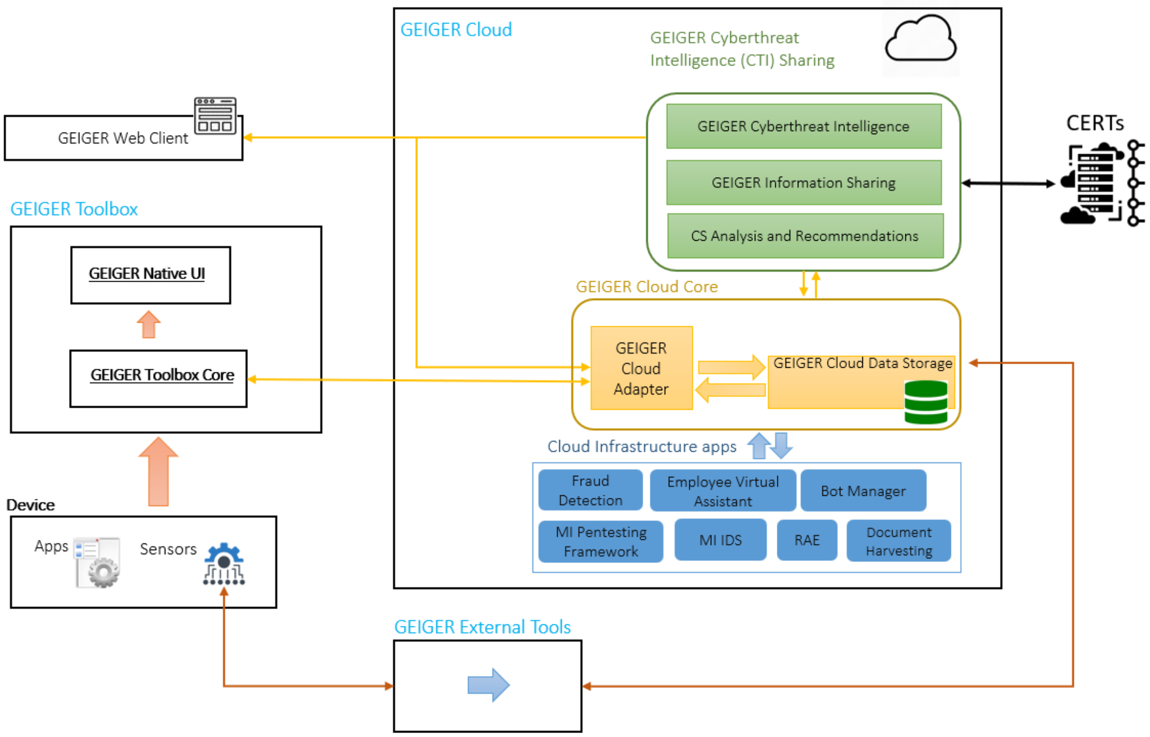

Figure 3: GEIGER detailed architecture

data exchange. The data model for the information stored locally includes various types of entities, such as:

- SME information, including
- Device information.
- Personnel information
- Global data, i.e., read-only data provided by the cloud.
- Keys, which contains the authorization credentials to obtaining end-2-end encryption (E2EE) data on the cloud.
- Local data, that is, information expected not to be cloud-replicated.

Privacy is a serious issue in GEIGER. Not only from the user-right protection side but also including authorization and sharing mechanisms. To manage privacy and protect the information, GEIGER implements a version of the Traffic Lights Protocol (TLP) which empowers the MSE by means of explicitly allowing businesses to indicate which information will be replicated in the cloud storage and which one should be kept stored locally.

Last but not least, the GEIGER Toolbox has another important component: it provides the UI or “GEIGER Native UI” for the interaction with the end-user of the platform. The UI performs various functions such as being a point of contact with the end-user or enable him/her to introduce data into the platform. It has been designed in a modern, simple, and friendly way.

3.3 Data exchange

Information exchange plays a key role in the GEIGER platform. Data must flow between the GEIGER Cloud and the Toolbox smoothly. This is achieved thanks to both the APIs developed (GEIGER Controller and GEIGER Cloud Adapter), whose endpoints supply and retrieve information upon request, and the Information Sharing Platform, which gathers data from security entities such as the CERTs.

The implementation of privacy, with the help of the Traffic Lights Protocol (TLP) protocol, makes GEIGER a solution reliable for MSEs, which can manage the amount of its data to be stored in the online storage at any moment. Therefore, GEIGER effectively deals with information, in terms of privacy and security.

Both the GEIGER Cloud and the GEIGER Toolbox have been designed and integrated as the core of the platform, meaning that every one of them performs their duties and complement each other.

3.4 GEIGER Indicator

The GEIGER architecture includes an algorithm which performs an automated cybersecurity risk assessment based on the data contained in the local data storage, upon request of the MSE user. The cybersecurity risk assessment results produced by the algorithm are presented to the user in the form of a score: the GEIGER indicator.

The GEIGER indicator algorithm is threat-based. Due to their limited cybersecurity resources, MSEs require a solution that is automated where possible and that can prioritize where necessary. This motivates the use of a threat-based cybersecurity risk assessment approach, since these methodologies have been shown to allow for automation [1, 3] and prioritization [4, 5].

It is widely recognized that different MSEs deserve different treatment in cybersecurity risk assessment approaches [5]. Therefore, we create threat prioritizations for MSE profiles based on characteristics such as country and sector. This is done with the help of incident data streams originating from CERTs connecting to the GEIGER solution, as indicated in Figure 1.

By incorporating live incident data from CERTs directly in its risk assessment algorithm, the GEIGER indicator can update based on changes in the cybersecurity threat landscape automatically. This ensures that the GEIGER indicator, and the GEIGER application, stays relevant to the MSE user over time. We hope the GEIGER indicator will drive user motivation to use the GEIGER application, through its automated nature, simplicity, and adaptability.

4 GEIGER ADDED VALUE

4.1 How can GEIGER help MSEs in today's challenging environment?

Nowadays any company faces a lot of challenges. Not only the obvious competitors of the market but also the security challenges that the internet world raises. Besides, big companies have the resources, expertise, and personnel to deal with those issues, but the situation is dramatically different for MSEs, which usually are made up of a few users and operate on a tight budget.

Considering all these factors, GEIGER can be a good fit to support MSEs smoothly and effectively in several ways such as:

- Contributing to increasing cybersecurity awareness on users. There is no magic formula that guarantees protection from cybercriminals, but GEIGER represents a huge step regarding how to best achieve a higher level of protection against threats.
- Providing cybersecurity training to untrained end-users and making them acquire a good set of cybersecurity skills.
- Handling and displaying updated cybersecurity information, including attacks, threats, vulnerabilities, exploits and whenever may be requested.
- Helping SMEs to better manage cybersecurity and, as a result, being more competitive in their market sector.
- Bringing cybersecurity over the MSE in a friendly and approachable way.

GEIGER effectively empowers the MSE in the various ways described. The ultimate goal is to make the organization more resilient when facing threats, especially if these are unknown.

4.2 What makes GEIGER an innovative solution?

Flexibility is one of the strengths of the GEIGER platform. The solution has been designed as a central piece that manages and effectively integrates various cybersecurity tools which enhance GEIGER capabilities. Regardless of the circumstances, GEIGER can adapt to different scenarios just by integrating new cybersecurity tools with few efforts. This ability to easily incorporate new pieces into the puzzle provides great flexibility to the platform and makes GEIGER suitable for different scenarios.

In addition, GEIGER makes use of its GEIGER Indicator to permanently provide the risk level status, keeping the user updated about any possible risk. Users are, therefore, more aware of any issue that may arise as soon as it is presented, which leads to better management of the security and the overall business.

5 CONCLUSIONS AND ENHANCEMENTS ON THE PLATFORM

In terms of cybersecurity, the only certainty is that there is no perfect protection. However, the GEIGER platform proposed entails a big step regarding raising cybersecurity awareness among MSEs, i.e., among users.

The architecture of GEIGER has been carefully designed to consider the various possible scenarios and situations that MSEs and their employees face nowadays. The possibility of being enhanced with new features and tools, combined with both its online and offline features, makes GEIGER a good choice to effectively deal with cybersecurity threats.

GEIGER also delivers frequent updates in terms of information exchange to be able to recognize and react to new threats forcefully. In this context, collaboration with CERTs empowers GEIGER, making it possible to keep MSEs updated and protected most effectively.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER).

REFERENCES

[1] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. 2019. Toward the Automation of Threat Modeling and Risk Assessment in IoT Systems. Internet of Things 7 (Sept. 2019), 100056. https://doi.org/10.1016/j.iot.2019.100056

[2] European DIGITAL SME Alliance. 2020. The EU Cybersecurity Act and the Role of Standards for SMEs - Position Paper. Technical Report. Brussels.

[3] Yang Liu, Armin Sarabi, Jing Zhang, Parinaz Naghizadeh, Manish Karir, Michael Bailey, and Mingyan Liu. 2015. Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In 24th {USENIX} Security Symposium ({USENIX} Security 15). 1009–1024.

[4] Michael Muckin and Scott C. Fitch. 2019. A Threat-Driven Approach to Cyber Security. Technical Report. Lockheed Martin Corporation. 45 pages.

[5] Richard P. Lippmann and James F. Riordan. 2016. Threat-based risk assessment for enterprise networks. Lincoln Lab. J, 22(1), 33-45.