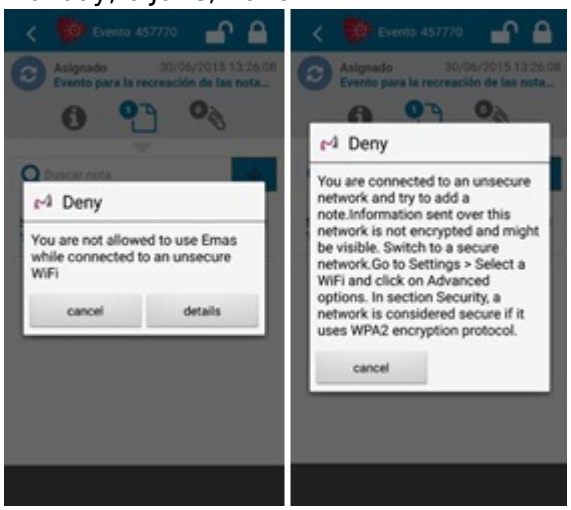
Published on *Horizon 2020* (https://ec.europa.eu/programmes/horizon2020)

Monday, 6 June, 2016



[1]

The user is perceived as the weakest link in IT security. More often than not risky user behaviour finds its roots in simple ignorance. The necessity to proactively engage the user on IT security has become acute with recent developments in the corporate world, such as the introduction of mobile technologies or the Bring Your Own Device trend. Project MUSES has developed the prototype of a software that provides security guidance to the user by offering real-time, context-based recommendations.

One illustrative scenario is that of an employee attempting to send confidential data over an unsecure network. In this case, the MUSES software automatically detects this risky behaviour and blocks the action. A pop up message explains the policy provision relevant to the action and guides the user so that he/she proceeds in a manner that is safe and compliant with corporate security policies. MUSES also operates at organisation level, by submitting the incident for evaluation to the IT Security department and by assigning a level of trustworthiness to individuals and devices, so it can be further used to allow or deny actions based on concrete trustworthiness thresholds.
MUSES reduces the number of security incidents in the organization, by providing the current security status of the BYOD (Bring Your Own Device, where employees use their personally owned laptop or mobile phone at the workplace) or COPE (Corporate Owned Personally Enabled) device and providing the user with feedback on his/her actions so he/she becomes aware of their potential impact.

In complement to the prototype, the MUSES project has drafted a full set of enhanced corporate security policies that strive to be more concrete and comprehensive than the policies standardly used in businesses, making it easier for the average user to understand and comply with what is expected of them.

The prototype was validated during trials conducted along two different business scenarios: a

consultancy department and a CSIRT (Computer Security Incident Response Team) organization. Feedback from the trials testified of a heightened awareness of corporate policies. Thanks to the materialisation in real time of the relationship between the actions of the user, the recommendations of the corporate policies and the potential security breaches, the MUSES prototype has proven to be more useful than any security awareness campaign.
An important feature of the MUSES software is that it safeguards the privacy and the productivity of the user. This is key for the acceptance of the user and ultimately for the effectiveness of the deployment of the MUSES solution.

The project is now completed but the MUSES consortium is now pursuing follow-up research and academic activities while a group of partners are working on commercialisation plans.
MUSES consortium plans for exploitation are to adopt the prototype for internal usage, applied to consortium members, fully evaluating the features and robustness of MUSES, as well as analysing employees' reactions to its daily usage. In parallel, the commercialization strategy includes:

- An open source version of the MUSES software that comes free, while support and deployment services are charged. The target market is that of SMEs and individuals.
- A business version of the MUSES software that is delivered under the "Software as a service" model and commercial license and consultancy services.

Muses was co-funded under the EU's Seventh Framework Programme for Research and Technological Development.

See also:
CORDIS [2]
Project:
Multiplatform Usable Endpoint Security
Project coordinator:
S2 Grupo
Project Acronym:
MUSES
Project website:
https://www.musesproject.eu/ [3]
Contact:
info@musesproject.eu [4]

Source URL:
https://ec.europa.eu/programmes/horizon2020/en/news/muses-software-greater-engagement-user-security-corporate-information-systems

Links
[1] https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/newsroom/muses_13834_0.jpg
[2] http://cordis.europa.eu/project/rcn/105550_en.html
[3] https://www.musesproject.eu/
[4] mailto:info@musesproject.eu