Battling Security Fatigue – Working Towards Usable Security

Security fatigue is not just an expression used by experts as an excuse for users who fail to comply with data security policies. The National Institute of Standards and Technology brought security fatigue to everyone's attention with a study which revealed that people with different backgrounds and jobs are tired and overwhelmed of updating their passwords, PINs, paying attention to security notifications, creating new accounts, reading privacy notices, adopting safe practices, etc. The study also revealed that the consequences of this phenomenon are, in most cases, the abandon of security protocols, the choice of the simplest paths, like ignoring the security guidelines, and, at the end, data security incidents derived from this behavior.

Security fatigue hits all industries, but especially financial institutions. The regulations and data security policies are stricter compared to many other industries due to the great amount of sensitive data collected, stored and processed. Employees are requested to frequently change passwords, to not use the same password for multiple accounts, to encrypt data, to constantly be on alert when working with customers´ financial records, taking much time out of their working hours and frustrating them because these daunting activities are perceived as out of their job description. It is no wonder that, despite the increasing budgets and implementations of cybersecurity tools, the breaches and incidents continue to make the headlines.

The solution to combat an "illness" that is caused by longtime practices is not simple. Changes need to come from the top-bottom, from the management to lower levels, and from vendors to organizations. Data security solutions must be redesigned to make things easier for users, to help them decide faster or to limit the number of decisions users need to make. Organizations are also responsible for instilling good security habits into their users. Financial institutions can take advantage of the resources they have, especially technical staff, to create awareness programs and to instill in people the advantages of following documented security procedures. Many users fail to respect security guidelines and end-up with the security fatigue syndrome because they do not understand why they are supposed to do so and what the consequences are if they don't.

Another method that has proven to be successful in other fields like education, sales and others, is gamification. Everybody's perspective can be changed when some fun and enticement is added to security. There are also some fast and in-hand solutions, like a password manager. While it is a simple solution to the endless and numerous passwords, many employees do not use it, because they do not know about it, or have not been informed. Insider threats become even more pronounced because of security fatigue – whether we're talking about IT teams or end-users. Yes, IT Administrators are also affected by this condition due to the multiple tools they work with, the volume of security alerts and information, reports they have to interpret, and issues that they must investigate and resolve.

continued on Page 2

Roman Foeckl
Founder & CEO

COSOSYS

Contact Info

www.endpointprotector.com

Roman Foeckl is the Founder and CEO of CoSoSys. Before founding the company in 2004, Roman worked for Goldman Sachs in Frankfurt, Germany and Paris, France. He studied business in Wiesbaden, Germany. After the acquisition of CoSoSys by Astaro and the subsequent acquisition of Astaro by Sophos, Roman together with Michael Bauner took the company private again in a Management Buyout (July 2011), with the goal to build CoSoSys and its Endpoint Protector product family in the leading content aware Data Loss Prevention (DLP) and Mobile Device Management (MDM) offering on the market. Roman's vision is to offer an easy to use and implement Data Loss Prevention Solution that covers all popular platforms, from Mac OS to Windows and Linux, so large and small businesses can protect their data against accidental loss or intentional data theft.

Battling Security Fatigue – Working Towards Usable Security

As a Data Loss Prevention vendor, we do not only have to minimize insider threats, but also make sure our product is intuitive, easy to use for Administrators, and non-intrusive for end-users. Our DLP product, Endpoint Protector 4, prevents data leakages by inspecting content being transferred to online services, applications, to portable storage devices, and other exit points and blocks the transference if sensitive data is found in e-mail bodies, attachments, uploaded documents, or even in Copy & Pasted content.

We make it easier for IT Administrators through predefined policies based on file type, on regulations, like PCI-DSS which are really useful for financial institutions, granular policies for devices, users, computers and groups, through a smart management console structure which has a short learning curve and many other UX tweaks. Alerts can be sent to the Administrators' e-mail addresses so they are not forced to constantly check the console.

Additionally, we offer a Mobile Device Management module within the same interface, so Administrators do not have to use two solutions to manage laptops, desktops and mobile devices. As for the end-users, we created two modes for the DLP module – Report only and Block and Report – with the goal of making it non-intrusive. With the Report only mode, users' content transfers are not blocked, just reported to the server, and they are only restricted if the IT Administrator, together with their management team, decide there was a policy violation.

Notifications that users receive can be hidden, to reduce the stream of information, although many organizations use them to raise data security awareness. We have also setup a customizable threshold that offers more flexibility when it comes to transferred data – e.g., a file can be sent by e-mail if it contains one Credit Card Numbers, but cannot be sent if it contains more than one.

To offer even more flexibility and make it more usable for IT staff and users, our DLP solution provides the option to create whitelists based on specific files, file locations, e-mail domains, URLs, or network share drives. This way, employees' productivity is not affected and security fatigue is reduced.

When it comes to reducing decision making for users, we also help through the EasyLock USB Enforced Encryption. For any USB device employees use to store data, our Device Control module with the EasyLock software automatically encrypts encryption on USB devices.

Security fatigue is a serious issue and it could get worse if data security is continues to be in the hands of IT security professionals only. Multidisciplinary teams at security vendors must work together to eliminate the pressure and the feeling of being overwhelmed directly at the source, in the product development process.

Roman Foeckl
Founder & CEO

COSOSYS

Contact Info

www.endpointprotector.com

Roman Foeckl is the Founder and CEO of CoSoSys. Before founding the company in 2004, Roman worked for Goldman Sachs in Frankfurt, Germany and Paris, France. He studied business in Wiesbaden, Germany. After the acquisition of CoSoSys by Astaro and the subsequent acquisition of Astaro by Sophos, Roman together with Michael Bauner took the company private again in a Management Buyout (July 2011), with the goal to build CoSoSys and its Endpoint Protector product family in the leading content aware Data Loss Prevention (DLP) and Mobile Device Management (MDM) offering on the market. Roman's vision is to offer an easy to use and implement Data Loss Prevention Solution that covers all popular platforms, from Mac OS to Windows and Linux, so large and small businesses can protect their data against accidental loss or intentional data theft.