Can an Early Warning System for Home Users and SMEs Make a Difference? A Field Study*

Urs E. Gattiker

CyTRAP Labs, Roentgenstrasse 49, 8005 Zurich, Switzerland
Critis06@CyTRAP.eu

Abstract. This paper outlines how early alert systems can help home users and SMEs in improving their security hygiene (culture of security). The viability of our framework and concepts are evaluated using www.CASEScontact.org as a case study. The latter offers its services to targeted groups of home users and SMEs supporting them in better protecting their information and data assets stored on, for instance, PCs or smartphones. As this paper shows, careful targeting of services (e.g., type of information and technical focus) and diligence (e.g., accurate and timely information is being provided) are a must for attaining users' trust and confidence. Only then may behavioral change follow that will, in turn, improve security hygiene (culture of security). As a result, we present conceptual and empirical evidence for the need to integrate marketing and information security elements to improve an early alert system's resource-advantage.

Keywords: awareness, critical infrastructure, critical infrastructure protection, crime, culture of security, cybercrime, CASEScontact.org, CyTRAP Labs, early warning system, EWS, freeware, identity theft, incident response, information assurance, information security, lessons learned, malware, phishing, patch management, prevention, public-private partnership, privacy, risk management, security assurance, security guide, threat, trust, US-CERT, virus, vulnerability, worm.

1 Introduction

In 2002, the OECD released a statistic that indicated that 4.9 percent of inhabitants had a broadband connection such as DSL, cable or ADSL. By 2004 this number had risen to 10.3 percent, while for 2005 the OECD reported a 13.2 percent average (EU15 = 14.2 percent) [1]. Based on June 2006 statistics the OECD reported that many countries in Europe have numbers in the high twenties (e.g., Belgium, Denmark & Switzerland) [2]. If we consider that a household may, on average, consist of two

* An earlier version of this paper was presented at the First International Workshop on CRITICAL INFORMATION INFRASTRUCTURES SECURITY (CRITIS'06) August 30 - September 2, 2006 Samos Island, Greece. A longer and more detailed version of this paper entitled "New threats and national warning systems - lessons to be learned" can be downloaded from http://cytrap.eu/blog/?p=30.

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 112 – 127, 2006.

people, it follows that in many EU Member States as well as OECD ones, 50% or more of a country's citizens have broadband access to the internet.

Also, a widely cited 2001 report by the CERT/CC [3] indicated that it had observed a significant increase in activity resulting in compromises of home user machines, specifically targeting those with cable modem and DSL connections. Recent data indicate that new type of threats than can spread ever faster continue to be a significant threat [4]. Unfortunately, home users have generally been the least prepared to defend against attacks, while often not updating their software or defence mechanisms as they should. Hence, detecting and resolving attacks on those systems is a real challenge.

For this reason, several Member States of the European Union and their representatives met with experts in July of 2002 to discuss how better awareness could result in improved prevention for home users and citizens, thereby being better protected against attacks. This resulted in the creation of the Cyberworld Awareness and Security Enhancement Structure or CASES for short (e.g., see CASEScontact.org, CASES-CC.org, and CASES.lu).

This paper tries to advance our knowledge of how early alert systems can help in improving prevention and security posture against malicious code and attacks for home-users and SMEs. This is accomplished by the application of generally accepted concepts that have been used regarding early warning systems for quite some time. The objectives of this paper are (1) to determine what structure must be used to reach target groups of users with warnings regarding threats, vulnerabilities and zero-day exploits, and (2) to assess whether such a tailored and targeted service (i.e., according to age, using different information distribution channels) can help in fostering better prevention by users to raise the protection level of their systems and data.

The article is organized as follows. First, the conceptual background is discussed; in particular, how an early warning system could help home-users and SMEs is outlined. Next, the requirements for an early warning system (EWS) to make it services valuable for home-users and SMEs are presented. Third, the framework offered is then analyzed using CASEScontact.org as a case study. Finally, we summarize key issues for early warning systems for home-users and SMEs, suggest ropes to skip and highlight management as well as policy implications.

2 Moving from Awareness to Active Defence

To reduce a health pandemic or the number of incidents caused by smokers falling asleep in bed, federal governments, public health offices and fire departments have, for a long time undertaken efforts to raise awareness about fire and health hazards. Hence, pamphlets and/or other information provide insights and checklists helping citizens to take the necessary steps for achieving effective fire prevention. Similarly, improving dental hygiene and reducing the spreading of infectious diseases requires that children are being taught early.

As well all know cleaning one's teeth regularly reduces the risk for dental decay. But this does not mean that we clean them them regularly after each meal as we should. Similarly, most users' know that one should refrain from just opening an attached file sent by somebody. This helps reduce the risk for having one's PC