Distributed security

June 15 2009

Could an entirely new approach to online security, based on distributed sanctions, help prevent cybercrime, fraud and identity theft? A report in the *International Journal of Intercultural Information Management* suggests it could.

Susan Brenner of the University of Dayton School of Law, in Dayton, OH, and Leo Clarke of the Thomas M. Cooley School of Law, in Lansing, MI, suggest that government could control cybercrime by requiring anyone accessing cyberspace to employ reasonable security measures but without infringing on civil liberties.

Modern criminal law has its origins in the industrial revolution of the nineteenth century and does not meet the needs of the current digital age, Brenner and Clarke explain. Currently, sanctions against criminals, such as prison sentences, fines, and the freezing of assets rely on a system that can entrap the criminals in order to bring them to justice.

As such, the law repeatedly fails to tackle the modern phenomenon of cybercrime, where criminals operate virtually through distributed networks and exploit a multitude of loopholes in software and hardware, and as ever through social engineering. There are many reasons that the old legal system fails to combat cybercrime, but primarily it is because the criminal can be anywhere in the world, all they need is an internet connection to commit many thousands of crimes at once.

The researchers say that a new paradigm is now needed to cope with this changing landscape of criminal activity. This new paradigm cannot rely

on sanctions, but must instead turn the distributed nature of cybercrime on its head.

They suggest that a new model must shift the focus of law enforcement from reaction and punishment to deterrence and prevention and to do so requires something akin to community policing but in the virtual world. Individuals must recognize that they are their own front line defense against cybercrime, but with the critical community structures that can exist on the internet they are not alone in building and maintaining their defenses, the researchers explain.

Fundamentally, Brenner and Clarke argue, a new generation of cybercrime prevention laws would require citizens, organizations, and companies to identify and obtain the tools necessary to prevent cybercrime, to install these tools and keep them updated, and to use them in an effective manner to prevent identity theft, anonymous email relaying, and the expansion of zombie networks of infected computers.

However, they do not provide a prescription for deciding which tools are effective or how this might be policed. Nevertheless, by inverting the usual prevention and sanction approach, the individuals' expectation of law enforcement becomes their responsibility to avoid being a victim.

Source: Inderscience Publishers (news : web)