

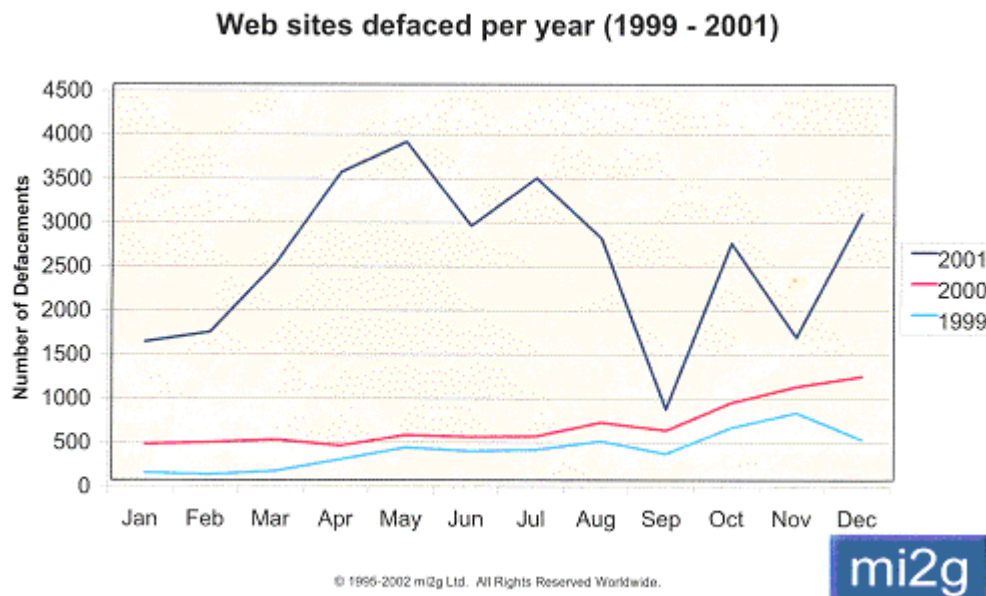
The changing face of web security

Introduction

In the 'real' world, computer technology has been led by ease of use and ease of operation. By comparison, computer security technologies have been identified as preventing rather than facilitating business. Unless computer security technologies make themselves easy to use, give the user information they can understand, give warnings that are relevant, and only impose restrictions when commercial imperatives insist, they will fail to deliver value-added security. If we examine the area of web sites we can get a feel for whether security is winning or losing.

Web site defacement

As a quick measure of general web security we can look at the published figures for web site defacements over the last few years. The research group mi2g published the following table for the years 1999-2001 based upon their own research.



A quick calculation suggests that over 30,000 sites were defaced during 2001, and there is no reason to believe that 2002 will be any different. If these figures do not disturb, the other respectable sources listed below bear out the worrying trend that mi2g have highlighted.

From The Computer Security Institute, 12 March 2001,
With the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, http://www.gocsi.com/prelea_000321.htm, out of 538 respondents (directly quoted):

- 85% (primarily large corporations and government agencies) detected computer security breaches within the last twelve months
- more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%).
- The rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001.

- 97% have WWW sites.
- 90% of those attacked reported [web site] vandalism (only 64% in 2000).
- 78% reported denial of service (only 60% in 2000).

From ZDNet, 24 January 2001,

<http://www.zdnet.com/zdnn/stories/news/0,4586,2677878,00.html>

"Failing to responsibly patch computers led to 99 percent of the 5,823 Web site defacements last year, up 56 percent from the 3,746 Web sites defaced in 1999, according to security group Attrition.org."

From Attrition, 4 Jan 2001,

<http://www.attrition.org/mirror/attrition/os.html>

"In a year and 4 month period, between August 1999 and January 4th, 2001, 8071 separate web sites were broken into and subsequently defaced."

Winning the battle?

It seems that the security people are losing the battle as well as the war. The Internet was designed to provide one of the three key security functions – availability, but not the other two, confidentiality and integrity.

The solutions that have previously been available to protect web sites may have protected some of the e-trade sites, but they are expensive to acquire and complex to implement, placing them out of the reach of the medium scale enterprise, never mind the small business and the wealth of small information providers that make up a huge proportion of the free information available.

The much publicized padlock on the browser has been disappointing. After years of pushing out the message that 'if it's there you know it's safe' most users still don't know what it's about. It never does anything, and as a result, neither does the user. It's the ultimate security secret weapon. It tells you nothing, and if you click on it the information you get is hardly meaningful. Far from being involved in the security, the message to the user is, "Keep out!"

New techniques, such as those being pioneered by E2 Labs(www.e2labs.com) which provide for low cost active protection may reverse the balance. Security people will tell you that the user must be actively involved, so a move towards publicly available solutions has a lot more going for it than the current industry approaches.

Losing the war?

Of course, the conventional approaches to security for web sites have to be considered. You see a lot of sites these days publishing logos. The user is expected to realize they should 'click' on the logos to see if they are real and to see what happens next. Unfortunately hackers can create logos and false lookup panels just as well as anyone else. Also, even if checks are made on web pages before they leave the original site, cached pages elsewhere can still be changed without detection and leaving the claimed security looking more than ragged.

SSL is a very effective technology for ensuring that information passing between two points on the Internet cannot be read by an attacker. (You can't, in version 2, tell if there is a man in the middle reading everything, so it isn't quite perfect. SSL does not protect the web site itself either, so it doesn't slow those hackers down at all.) The other downside of SSL is the sheer machine expense of running it. Encrypting pages from the web site every time they leave costs a lot of machine processing that would be better used giving response time to customers.

Setting it up if you are the web site owner is quite another matter. To do that, apart from having to do some rather arcane programming, which hopefully the programmers get right, you need a 'server certificate'. Getting a server certificate (or indeed any other form of digital identity) is an interesting experience. There are quite a few suppliers of such products, BTIgnite, Geotrust (including Equifax secure), TrustDST, GlobalSign, THAWTE and VeriSign to name but a few. The web sites advertise many products and services, but you need to be an expert to understand what it is that you are buying and how you are going to use it. That probably works fine for the IT departments of big business and the major portal providers, but the ordinary business is likely to be sunk without trace.

A major re-appraisal of Certification Authority (CA) sites is needed if they are ever going to appeal to the public. The average user will take a few moments to look at all the strange language before switching rapidly to a search engine with more useful content. Even if they do progress to the detail, many of the explanations all assume that you already know what you are doing and how it is supposed to work. How the normal mortal chooses between national, global, super, code and however many other types of certificates is open to question. Does a web site need a server certificate or will a Class 3 personal do the job? And why? After all, the great majority of web sites they know nothing about the server, they're being hosted from an ISP who might know some more of the answers.

The changing face

Whatever happens, it will change the face of web sites. Security sites are going to have to learn to appeal to their customers, and speak the customer's language – not expect the customer to learn security-speak.

Web sites are also going to have to change. The current protection methods of checking pages as they leave a site gives no protection to customers. Customers also need active software on their desktops telling them when there's a genuine reason to worry, not passive padlocks leaving them to guess when they should do something, and when they do, leaving them so confused with security jargon that they can't tell right from wrong. At the moment, to quote Samuel Smiles, "The cure is worse than the disease."

Security itself will also have to change. The issue is not how to convert users into security experts and seeing things from a security perspective. The issue is how to convert security experts into talking to users in user language and seeing problems from the user's perspective.