Managing the Risk of Web Security

Author: Henry Harrison, Co-founder & CTO of Garrison Technology

GLOBAL RISK INSTITUTE

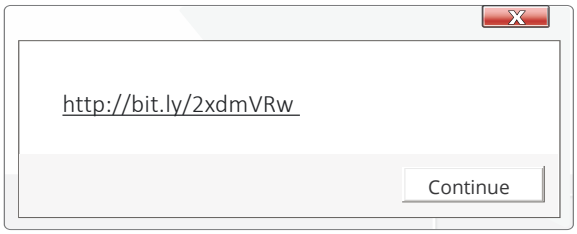
The author is an independent contributor to the Global Risk Institute and is solely responsible for the content of the article.

UNDERSTANDING THE RISK FROM THE WEB

When you click on a link, you invite whoever set up the server it points at to send you all manner of code to be executed on your device. They then invite all manner of "partners" (for example, advertising and analytics companies) to pass along the code they want to send you. All this unknown code then gets processed by the software running on your device to display everything from a paper on the latest breakthrough in artificial intelligence to what a Kardashian ate for breakfast.

You certainly have no idea who all the "partners" are, and much of the time little or no idea who set up the server. You don't know if their intentions are benign or malicious, and you have no idea whether their security practices are good enough to keep out other malicious parties that might try to compromise their server and put their own data on it. You have very little idea what country the server is in, and in most countries, there is very limited effective law enforcement to dissuade a malicious party from sending you malicious data.

WOULD YOU CLICK THIS?



Put like that, it is a miracle that the impact of web-based malware is not even worse than it is. For that we must thank – predominantly – the heroic efforts of browser and Operating System developers who go to great lengths to minimize the risk that if someone does send you malicious data, dreadful things happen. So, most of the time, you click on a link and nothing goes wrong.

But the risk is far from zero. For example, until September 2018 any browser running on Windows was vulnerable to a web page containing a malicious image. Anyone who clicked on a link to such a page could have their Windows PC compromised by whoever created that image – and that could lead to very bad things: ransomware, data breaches or financial loss. There is no doubt that many, many more such vulnerabilities remain, yet undiscovered. And of course, more get added all the time, as part of new software or updates.

COMMON CYBER THREATS

THE STATE OF WEB SECURITY TODAY

As a result, companies have invested in a wealth of additional web security tools. But at heart, for more than two decades, these have all worked in the same way: they try to identify malicious sites or data and then block them.

Unfortunately, the cyber threat never stays still, and this approach is now creaking at the seams. There are two primary reasons: firstly, increasing technological sophistication on the part of cyber attackers, whose primary aim is to avoid being identified as malicious. But secondly, where organizations are concerned, the risk is not only of being caught in the crossfire by a malicious site that will attack all comers. Potential adversaries are now targeting specific organizations, so that a site may be entirely benign for everyone else, but malicious for a visitor from that particular organization. In this case, it is very hard to identify the site as malicious until it is too late.

Leading companies are now moving beyond the traditional approach of blocking sites that are known to be malicious and instead starting to block sites if they pose a risk of being malicious.

Clearly, this new approach relies on a risk assessment. Some companies are buying in that risk assessment from specialist threat intelligence providers. Others are developing their own risk metrics based on criteria like the country a server is in; how long the server's domain has been registered; or whether traffic to the site is encrypted.

The good news is that a massive risk reduction can be achieved with only a limited impact on the user base. There is a clear correlation between frequency of visits, and associated risk: the most popular sites such as Google pose a comparatively low risk, while the highest risk sites are obscure and rarely visited. It is possible to block a large proportion of the risk while affecting only a small proportion of an organization's browsing.

SECURITY VS USABILITY

But even a small number of blocked sites can be infuriating for a user who is trying to get their job done. In the 21st century, employees are knowledge workers, and blocking their access to information can have significant business impact. As is so often the case, risk reduction will only be possible if the business impact can be mitigated.

Many organizations have an "exception handling" regime that allows users to request access to sites that have been blocked. But there is little risk-based thinking behind this approach and in many cases, it represents the worst of all worlds: such processes rarely if ever say no to an exception request, thus introducing a road bump for users that causes significant annoyance and inefficiency while invalidating the original risk reduction strategy.

Better approaches rely on providing lower-risk means for the user to gain access to otherwise blocked sites. The most common approach is for the user to use a physically separate device. Some will provide users with separate "dirty" machines that have a less restrictive blocking policy, but much more frequently, users dig out their personal smartphones connected to 4G or a Guest Wi-Fi network and use these to bypass security policy and get the job done. Some will even start working from home where their personal IT does not suffer from the same restrictive policies.

NEW SOLUTIONS

Other organizations are looking for a more satisfactory solution that will allow users to gain access to the information they need, using their regular computing device – but without putting the computing device (and the systems and data it has access to) at risk.

Such a solution sounds like a mythical magic bullet. Given the effort that browser developers such as Google and Microsoft pour into trying to ensure their browsers can cope with malicious data, what trick are they missing? Any such solution will need to represent a dramatic technology innovation rather than simply "more of the same".

The answer is to use a trick: to use a physically separate machine to do the risky browsing, but to give the user control over that machine from their regular computing device.

This is not a new idea: many government organizations have been using this approach for over a decade with traditional technologies such as Citrix®. But experience shows that these traditional technologies scale poorly, and that residual security vulnerabilities mean the risk is not as far reduced as the organizations implementing them had hoped.

As a result, those governments are now turning towards new technology that uses hardware-level designs to ensure that the physically separate machines doing the risky browsing truly are isolated from the user's regular computing device. Users can gain access to information even on the riskiest websites while the organization's systems and data remain fully isolated from the risk.

What is perhaps surprising is that this hardware-level technology is not a specialist ultra-high-cost security solution suitable only for Top Secret government organizations. The same technology is being used by mainstream commercial organizations to provide isolated web browsing that enables a massive risk reduction, at a reasonable cost and with minimal impact on users.

Sophisticated and targeted cyber-attacks are not new, but in the early days of the Internet both their perpetrators and their targets were military and national security organizations. Today the pool of attackers has increased, as criminal and politically-motivated groups have increased their sophistication. And both they and the original nation-state attackers are now attacking not only governmental targets but also mainstream commercial organizations. The requirements of the two markets are converging, and a new generation of solutions is emerging: secure enough to protect against threats that historically only affected government organizations, while scalable and at a price point that meets the needs of the mainstream commercial world.

PRACTICAL STEPS

Web filtering policies were originally driven predominantly by Human Resources and compliance considerations: for example, preventing access to content types considered inappropriate for access at work. Implementation of these policies usually fell to the Information Technology department. In response to the growing web threat, it is critical that responsibility for web filtering policies falls within the remit of risk and security professionals.

Organizations should then review options for risk-based blocking. This includes both data sources – for example, the use of specialist threat intelligence feeds versus category-based blocking – and organizational policy. It is likely that some departments or category of employee (those with access to particularly sensitive information or systems, or those with elevated privileges) should be subject to more stringent blocking policies.

Finally, organizations should review technological options to securely re-enable an otherwise blocked website. Any such review should look for clear evidence to back up vendor security claims: technology evaluations that focus on features rather than security claims can easily end up delivering little overall benefit and could in the worst case even deliver an increase to overall risk.