E&C - online privacy inquiry

Summary of Key points

Security of a system and its information goes to the very heart of privacy.

Without DMZ protection the security and privacy of any system or network has a substantive risk of breach. This risk is magnifying at exponential rates with the explosion in new forms of appliances, smart phones and computer technology.

USA Department of Homeland Security cites DMZ technology as best practice.

Until the development of Australian technology, DMZ protection worldwide hasn't been available for most organizations. Expense, complexity and time required to establish have all been major barriers.

Traditional VPN used by the majority of individuals for remote access to their online systems is insecure and weakens security.

Coupled with DMZ technology is a new standard for the security of remote access, extraction of information and reporting information.

New Australian technology allows DMZ technology to create a heightened fabric of security and privacy for all Australians.

All future development of software and applications in any particular industry including education should be carried out with DMZ technology in mind as a standard for privacy enabling technology.

We recommend an annual audit point on computer vulnerability for all entities operating in the education industry be deployed. This could also apply to the Financial Services Industry.

We also recommend a central register requiring the declaration and recording of all unauthorized cyber access episodes be established for the education industry.

We strongly endorse privacy by design and the embedding of privacy into the architecture of technologies and business processes from the outset.

Our company has identified a major worldwide problem with the security and privacy of information which we wanted to bring to your inquiry's attention...

This problem is the lack of availability of DMZ network protection for most organizations and individuals.

USA Department of Homeland Security cites DMZ network protection as best practice and the new PCI.

International credit card standard has from the 1st January 2011 referred to DMZ technology in its audit question guide.

Effectively DMZ's removes all direct interaction between trusted systems and the public internet for both inward and outward bound traffic.

Unlike firewalls DMZ's also utilize the principle of separation and interdependence to ensure a security standard applies to all the services interacting with the public.

It is the lack of application of the previous two principles which largely leads to the exploitation in the education environment of weaknesses by techno savvy individuals intent on unauthorized behavior.

DMZ technology has not been available for universal deployment until very recently.

Cost, technical complexity and the length of time to establish have all been prohibitive.

Most small to midsized organizations have been without DMZ protection and the integrity and security of their data venerable to unauthorized access.

Most firewalls can be penetrated by an average aged teenager using free downloadable software readily available on the internet.

Non DMZ protections deployed often do not recognize interdependence and weak points which allow unauthorized access. The security fabric needs to apply to all services and participants in a particular environment.

Password and logon protections are no longer considered reliable or effective. Software vulnerabilities and high powered technologies can facilitate ways to crack application level security making the question associated with non DMZ cyber security a matter of" when" not "if".

iwebgate have found over 90 percent of the organizations consulting ourselves can be breached, this is of major concern .Testing for access vulnerability is not an expensive or difficult process .We recommend consideration be given to the inclusion of a regular annual test as an audit point for all entities operating in given industries. Education being one of these.

Further because of the significance of cyber security in the education sector we would counsel the establishment of a federal register requiring declarations of all and any breaches to cyber security and privacy. Such disclosure obligations are common in major countries such as the USA, Germany and the United Kingdom.

I will attach a brief overview of the problems which underpin the reasons why our Australian company has developed DMZ technology to a level which all organizations no matter how small can access and apply as a new standard in privacy enhancing technology. Issues around cloud computing are also discussed in the attached brief overview.

I also confirm iWebGate has a contract pending with the USA Government and we understand that Washington has briefed our Prime Minister's office on the contribution this new technology can make to security and also network capability.

We are happy to speak by telephone and provide further information should your members require such.

Kind regards
Kim
Kim Mettam
Director of Business
iWebGate Pty Ltd