

Choosing a hosting provider you can trust



Contents

Choosing a hosting provider you can trust	4
Network Security	6
Server Security	8
E-Commerce Security	10
Physical Data Security.....	11
Zen Internet	13
Putting it all together	15

Choosing a hosting provider you can trust

For most UK businesses, online hosting has now reached the status of a basic utility – a service used day in, day out to project an image, provide information to customers, share data between the company and its employees, or even sell goods direct. From the smallest, sole-trader enterprise to the largest corporation, hosted websites, leased servers and rented data centres have become part and parcel of the way we do business today.

Unfortunately, choosing a hosting provider is far from easy. The market is saturated with products and providers, ranging from bargain-basement shared hosting packages through virtual dedicated hosts, physical servers and enterprise-grade, fully-managed services. Some providers take the 'pile 'em high and sell 'em cheap' approach, while others offer premium bespoke solutions with fearsome monthly fees. It's possible to sink hours into comparisons of server specification, bandwidth allowances, disk space and monthly costs, but sometimes a more important factor can be forgotten: how do you choose a hosting provider you can trust?

Why is this so vital? Simple. Even if the needs of a business only go so far as having a basic presence on the web, it's essential that that website stays accessible, and that it isn't compromised by image-damaging graffiti or subverted by hackers so that it becomes a home to malware. If your needs extend to e-commerce or customer

Meanwhile, more and more companies are now putting parts of their business out of house and online. In some cases, they're using hosted databases to share business information across an organisation or with trusted partners. In others, they're renting server space or rack space to host bespoke applications and hardware that their employees need 24/7 access to. Hosted servers may even be used to develop new Software as a Service (SaaS) products, or provide the means to deploy them to employees or clients. The benefits are obvious, but sadly, so are the risks. A business needs to be sure that the information on that server stays on that server, that the server remains available, and that the data can't be corrupted, stolen or accessed by unauthorised parties.

No hosting provider, no matter what they promise, can 100% guarantee these things, but without a hosting provider you can trust, there are no guarantees whatsoever. A good hosting provider isn't just selling you a product; they're selling you a service. While they might not be able to remove all elements of risk, they can take steps to minimise them and effectively negate them.

These risks are not decreasing. Of the 2,337 sites harbouring malware that Symantec's Internet security specialists discovered daily during Q3 2009, 80% were legitimate websites that had been compromised by hackers*. Vulnerabilities in the web server software or scripting applications, SQL Injection attacks and malicious advertisements are responsible for some of these, but some come down to attacks on the back-end infrastructure of hosting companies. Even the biggest

A business needs to be sure that the information on that server stays on that server, that the server remains available, and that the data can't be corrupted, stolen or accessed by unauthorised parties

support applications, you need to know that your site is secure. Malware or Denial of Service (DoS) attacks can cost you revenue, and if you can't trust your provider, then how can your customers trust you? If you're handling their data, then you need to know that that data is safe. In some cases, you may even be under legal obligations to ensure this.

names are not immune. In 2009 visitors to the New York Times website were endangered when hackers compromised the third-party ad servers supplying advertisements to its pages. In the last year, sites belonging to MSN Canada, Sir Paul McCartney and the UK Parliament have been successfully attacked.

How, then, can your business find a hosting provider you can trust? What features or services should they offer? What questions should you be asking of them before you sign up? This white paper aims to provide the guidance you need to make the right decision.

For our purposes, we're going to divide web hosting packages into five main types, though, as always, there are a few grey areas.

Shared hosting:

The customer leases hard disk space, services and a given quantity of bandwidth on a server that will be shared amongst multiple customers. This is by far the cheapest way of getting an online presence, but the fact that you're sharing hardware and in constant contention for memory, processor and network resources means it's not an ideal solution for anything more than personal, blogging or small business use.

Virtual dedicated hosting:

A single server with a dual core or quad-core processor is split into several virtual servers using virtualisation software, with each virtual server allocated a maximum amount of memory and hard disk space. Each virtual server still has to contend for processor and network resources with the other virtual servers installed on that machine, but – providing the servers are configured properly – you can expect something closer to dedicated server performance.

Dedicated server:

The customer leases a complete server box, provided and cared for by the hosting provider and connected to their network. The customer has complete control over the server and the software installed on it, but also full responsibility for the online security of the server and the management and updating of its operating system and applications.

Managed server:

The customer still leases a server, but the management, security and updating of the operating system and core applications on that server become the responsibility of the provider. In effect, the business is paying the provider to handle the fundamental technical issues, and provide a platform on which the customer's own engineers or third parties can develop and deploy the software solutions they require.

Colocation:

A service where the customer locates some of its mission-critical hardware within a data centre belonging to the provider. The provider provides a secure premises, rack space, network security and the network infrastructure, ensuring the smooth running of the customer's own hardware. This saves the customer the expense and bother of maintaining its own secure facilities, and alleviates stress on their own network.

As we'll see, each form of hosting brings with it its own issues and demands, both for the user and for the hosting provider. Remember that while some solutions appear to save you money upfront, that could become a false economy in time.

*Symantec's Q3 2009 MessageLabs Intelligence Report.
<http://www.messagelabs.co.uk/intelligence.aspx>

Network Security

The network is the first and most important piece in the security puzzle. If your prospective hosting provider doesn't take adequate measures to monitor and guard their own networks, and so the servers on those networks, then they are leaving an open goal for hackers and malware authors to steal or destroy information, subvert your websites for their own purposes, or simply prevent the applications installed on your server from doing their job.

First, let's look at the threats that your hosting provider needs to be guarding against.

Unauthorised access

The obvious one is unauthorised access. If an unauthorised user can infiltrate the network and gain access to the servers connected to it, they can either copy data from it, stealing, for example, customer information, confidential reports or credit card details, or they can simply alter or destroy files in an act of mindless or targeted vandalism.

Subversion

Next comes subversion – the modification of a legitimate website for purposes that might range from simple graffiti or vandalism to its infection with malware so that any visitors are attacked by what's known as a 'drive by' attack. As this is primarily a software issue, we'll cover this in more detail later on.

Any potential hosting provider who tells you that a single security appliance or software firewall will safeguard you against these threats is either naïve or disingenuous. The fact is, it takes a carefully layered approach to cope with all these threats. You need a full range of controls, monitoring services and policies in place, plus a staff trained to use them, so that if anything suspicious or potentially harmful is thrown up, it can be recognised and dealt with straight away.

Of course, a good firewall is a fundamental element, but don't assume that one host's 'firewall' will be as good as another's. Ask questions. First, how does your hosting provider have its firewall or firewalls configured? Do they use a single firewall as a bastion, providing protection only at the perimeter of the network, or do they back that up with additional firewalls or security appliances operating over distinct zones to ensure maximum security. Who has control over rules and exemptions? Is this something that your provider's customers can configure themselves and – if so – is anyone checking to ensure that security risks aren't being introduced?

Does your potential hosting provider rely on a software firewall application running on a general-purpose operating system, or have they splashed out on dedicated hardware? The former approach can be more cost-effective, resulting in savings for you, but if the operating system isn't 'hardened' properly against attack, the firewall itself could be the first point of failure.

Any potential hosting provider who tells you that a single security appliance or software firewall will safeguard you against these threats is either naïve or disingenuous.

Denial of Service

Finally we have DoS, where an attack is orchestrated on a network, or on a server or servers attached to the network, in order to prevent that site from functioning properly. DoS attacks have been around since the early days of the Internet, but recently they have been employed for financial, political, criminal and even espionage purposes, if the rumours about this summer's attacks on Korean and Baltic nation websites are to be believed.

If they are using a hardware firewall or a dedicated security appliance, try and find out some details. Do they surround their servers with a ring of enterprise grade security appliances, or is the network reliant on a handful of cheap appliances that will instantly become a bottleneck in the event of a DoS attack? In some cases, a slow firewall can be more of a risk here than the network it's protecting. Does the appliance inspect the contents of the application layer of the IP packet? If not, your hosted databases and applications, while not necessarily vulnerable, are certainly more open to attack.

Is Anti-Virus integrated with the firewall, or does your hosting provider rely on server-side software for that job? Software on the server can handle the task, but the integrated approach can provide superior performance. The best devices use custom ASICs and operating systems designed specifically to inspect incoming and outgoing packets and check data on an application level without compromising network speeds. That's why they cost more, but that's also why they're worth the extra money.

Again, a smart hosting provider relies on layers of security rather than a single point; taking a simple packet-filtering based approach to deflect the majority of simple attacks away from the network perimeter, then relying on more complex stateful inspection, proxy or application-based systems to provide deep protection closer to the servers.

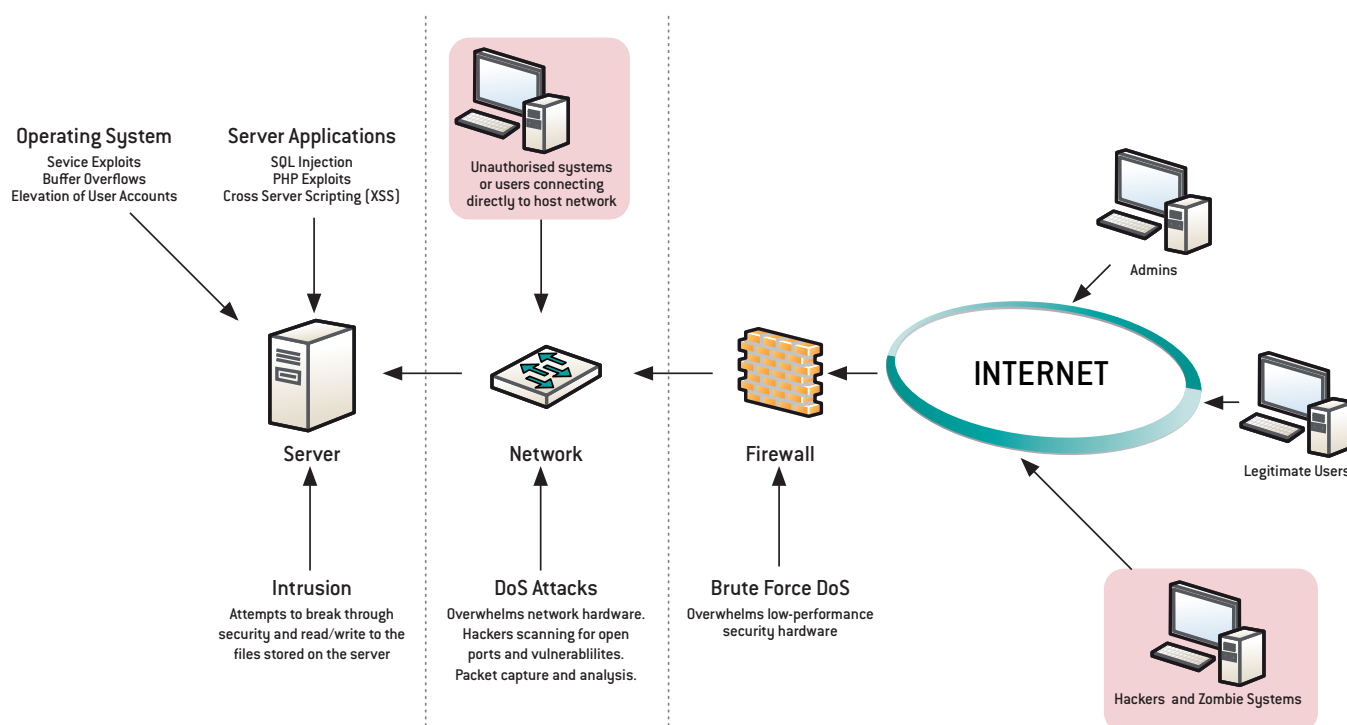
Not every customer needs hardware intrusion detection – a system designed to recognise and prevent unauthorised access and such malicious behaviour as the modification of applications and operating systems or the suspicious escalation of user privileges. In fact, as Intrusion Detection Systems (IDS) have to monitor all packets running through specific choke points in the network, there can be negative effects on performance should a hosting provider deploy it willy-nilly. That said, if you're trusting your provider with business-critical data then it's worth asking them whether it's an option, and what the associated extra costs might be. While you can't expect a bespoke service on a budget price plan, you should expect a hosting provider offering dedicated servers or,

particularly, managed hosting or colocation, to be willing to talk through your requirements and your concerns, and find a solution that fits you.

If you're looking for someone to host a business critical, confidential database or application, find out what appliances and protocols they use to provide Virtual Private Network (VPN) access. Secure Socket Layers (SSL) encryption is perfectly adequate for most needs, and simpler to set-up and manage, but in some specific applications you may want to ask if they offer the more secure Internet Protocol Security (IPSec). If you need VPN access across a large number of employees, you might also want to check whether there will be any limitations on concurrent user numbers due to bandwidth or VPN port restrictions.

Above all, secure hosting isn't just about software and hardware – it's about having the right people and policies in place. Ask your provider how closely they monitor the network; a good one has it watched constantly by people who have the experience to spot a suspicious spike in traffic, and the skills to deal with it should it turn out to be a DoS attack. They will also be monitoring the firewall logs to see who is probing the network for vulnerabilities, and whether there are any new tricks being employed to find a way in.

Common Attack Vectors



Sometimes the worst happens. Find out what policies your provider has in place in the event of a security breach, and what steps they will take to isolate affected servers or portions of the network should that become necessary. Is there a system in place for prioritising security issues? Even a team handling managed servers will be dealing with a range of operating system, application and user-account support requests at any time. You need to know that, should a security breach occur, that that alert will jump straight to the top of the stack.

Be aware that many security measures will depend on the package you choose, so don't be afraid to ask. With shared hosting packages some form of firewall will be a given – the hosting provider controls the operating system and software, and has it in its best interests to ensure that the websites running on its shared servers are malware-free. With a dedicated or virtual dedicated server package the provider's responsibilities end with providing the physical box, the operating system and the network, so it could be up to the customer to install appropriate security software – though a firewall may still be available as an optional extra. With a managed hosting package, firewall protection should be part of the service. Ask your potential hosting provider for details of exactly what they provide.

Cross-site Scripting (XSS):

A website vulnerability where an unauthorised script is injected into a legitimate website, where it subsequently sends malicious code in the form of client-side script to that website's end users. The script may be based on Javascript, HTML, Flash or any other form of code that might be executed by a browser. The big danger is that, to the browser, the code works within the security conditions of the website that unwittingly hosts it, giving the code access to read, modify and transmit any data, no matter how sensitive, that is accessible to the browser.

PHP Remote File Include:

An application vulnerability where specific functions in the scripting language give hackers a back-door to execute arbitrary code on the server. This can give them access to login information, or all the privileges needed to deface a website, introduce malicious code or gain access to the server as a whole.

Defending against these attacks is partly a question of following good coding practices within your own organisation. For example, by coding SQL inputs in terms of what can be included rather than what can't,

According to the System Administration, Networking and Security (SANS) Institute, attacks against web applications constitute more than 60% of total attacks seen on the Internet, with application vulnerabilities far exceeding those native to the Linux and Windows operating systems*

Server Security

Even with firewalls and security appliances in place, securing and maintaining the security of your hosted websites or servers is a serious issue. This doesn't just mean securing the operating system, but also the applications running on it. According to the System Administration, Networking and Security (SANS) Institute, attacks against web applications constitute more than 60% of total attacks seen on the Internet, with application vulnerabilities far exceeding those native to the Linux and Windows operating systems.*

The chief forms of these attacks are:

SQL Injection:

The hacker exploits security vulnerabilities within the SQL database employed by an application to introduce malicious code into that application. SQL Injection can be guarded against through tight coding, but it only takes a slip to give hackers a back door.

you can close down the vulnerabilities that allow SQL Injection attacks to succeed. However, it's also true that the majority of server-side attacks exploit emerging vulnerabilities in the most commonly used web applications, over which you will have less direct control. This makes updating and patching a major issue. Of course, if you use a dedicated, colocation or virtual dedicated hosting package, that responsibility is primarily yours. If, however, you use a shared or managed hosting package, then this responsibility will be shared or even handled solely by your hosting provider.

Ask your hosting provider whether they have a patching and upgrade policy? How are those upgrades staged? Are patches tested carefully before they're applied? Are security updates, which should be applied rapidly, handled differently to feature updates, which generally require more long-term testing? A good hosting provider engages in dialogue with its customers over these issues, informing them of major changes and how they might

*SANS Institute report. The Top Cyber Security Risks, published September 15th 2009

affect existing applications, content or databases installed on the hosted servers. A bad hosting provider either patches without due care, or lags behind. Be careful, too, of any provider that ignores major feature updates. While you might be able to do without new or revised features, you may find that future security updates will not work reliably on older versions.

While applications take the brunt of hacker attacks these days, Operating Systems remain vulnerable too. A good hosting provider hardens the operating systems on its shared and managed server packages, removing any tools, applications, services and administration features that pose an unnecessary risk and configuring the OS so that it's up to date and as secure as it possibly can be. Many operating systems come pre-configured more for ease of access and initial set-up than security, so this is a vital step. Don't be afraid to ask your hosting provider what steps they take.

Good security also starts with strong password authentication and control over server access. On a managed package your provider may well enforce strong password and user name policies, making it more difficult for crackers to gain login details through systematic brute force attacks, but on other packages look for a hosting provider who provides advice on user name and password security. If they support you, then they will also be supporting other users, and the stronger precautions those users use, the more secure the host's network as a whole will be.

Similarly, ask your hosting provider whether they provide secure log-in and file transfer facilities, either through SSL encryption or VPN. In certain situations you may need to log on from a site that is not secure enough for comfort, and it's good to know that your own login details are not being traced or stolen. Finally, ask your hosting provider whether they employ lockout thresholds on the hardware or operating system for password entry. Again, these can help protect against brute force cracking efforts.

It's always worth asking who on your provider's internal network will have access to your servers, and what privileges they will enjoy. On a managed package, this might come down to named individuals on your own support team, while on a dedicated or shared package there might be more widespread access. Generally speaking, the fewer employees with admin access to your server, the fewer attack vectors that hackers or unauthorised users will have to exploit.

Virtual dedicated hosts are becoming more popular, and it's not hard to see why. Theoretically, they offer much

of the power of a dedicated server at a price point closer to a shared package. However, not all virtual dedicated packages are equal, nor necessarily as secure as their physical dedicated equivalents. In the worst case scenario they can combine the disadvantages of a shared package with those of a dedicated box.

Why? Firstly, and as with a dedicated package, the onus is on the user to secure and maintain the server, its Operating System and the applications running on it. However, as with a shared package you're sharing the physical hardware with other customers. This can mean that a DoS attack which affects one virtual server can also affect other servers running on the same physical box. It also creates a risk – and there are established cases – where hackers exploit a vulnerability in an application running on one server to compromise that system, then go up to the physical hardware layer to attack other servers on the box. You can trust your host, but can you trust these other users too?

The trick is to understand that there is a difference between 'host based' virtualisation and what we call 'bare metal' virtualisation. In the first case, the hypervisor controlling the virtual servers works on top of the OS controlling the physical hardware. In the second, the hypervisor is working directly on the hardware, with the server OS running on top.

With host-based virtualisation, the 'hosting' operating system is a vulnerable target; if it's compromised, the attackers can reach any other servers running on that hardware. With the bare metal set-up, that window is firmly closed, making them intrinsically more secure. If you're interested in a virtual dedicated server package, ask your host how they provision it, and ask them what controls they have in place to regulate traffic between virtual servers, and ensure that heavy network traffic (or a DoS attack) affecting one server won't affect other servers running on the same hardware. By doing this it is perfectly possible to make virtual dedicated servers secure and reliable and therefore a viable option between shared and dedicated servers.

Finally, it's always worth asking your potential hosting provider what policies they have in place in the event of a server security breach. Do they instantly isolate the server in question? Do they attempt to fix smaller issues like a minor malware infection, or do they go for a brute-force wipe and reinstall? Do they refuse to reconnect servers or websites unless the cause of the security breach is addressed? What kind of support do they provide? If you use a managed or dedicated platform, find out what happens if your server is effectively destroyed. What

procedures does your provider have in place to restore your backups? Do they offer substitute servers that can get your business back up and running asap. A rock-solid hosting provider will have answers to all these questions. A cheap and cheerful choice might not.

E-Commerce Security

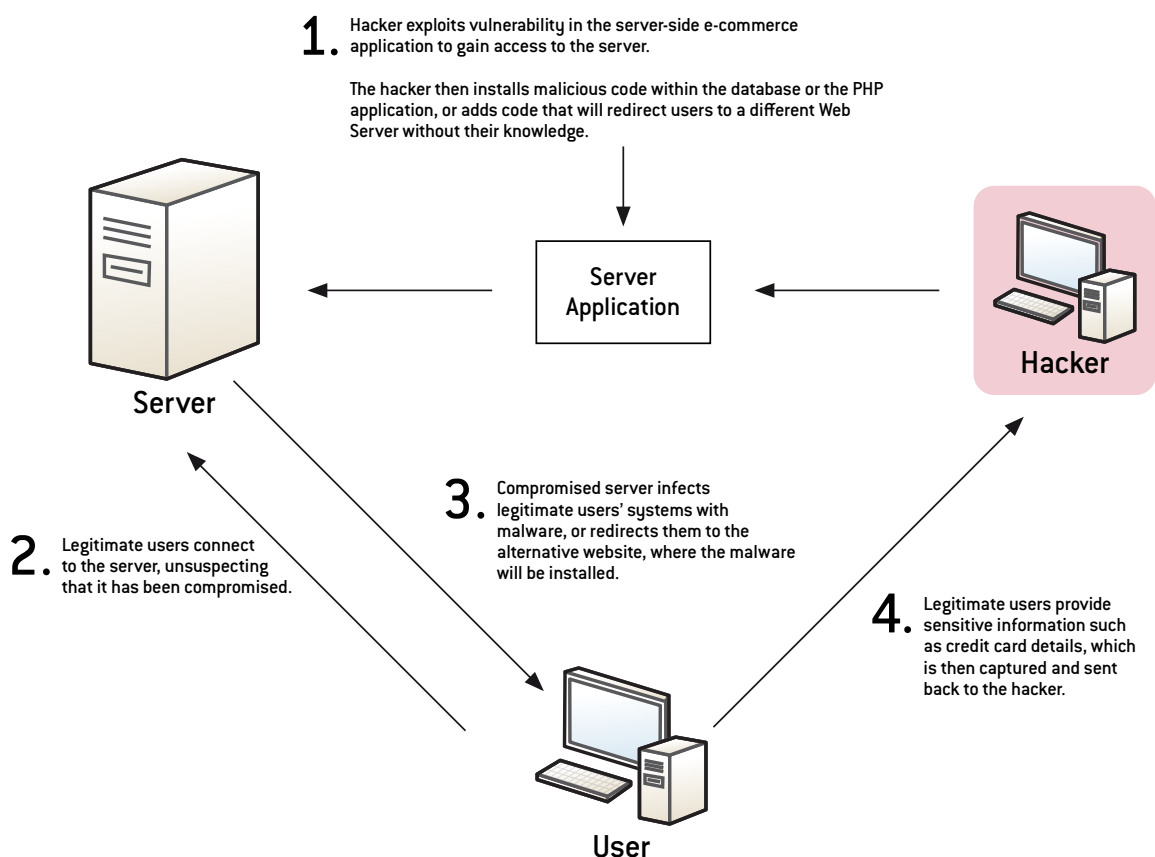
If you're planning to rent a server or shared space for e-Commerce applications, then security is all the more vital. For one thing, securing your site and your customer's data is plain good business sense; you don't want to be targeted by fraudsters, and any publicity pertaining to stolen customer or credit card data can be enough to close a business, practically overnight. While smaller companies are unlikely to face the sort of £3million fines and national outrage that resulted from HSBC's security breaches in 2009, where unencrypted discs containing customer data were lost in the mail, there are still consequences.

For example, in 2008 it was discovered that an online store affiliated with the UK's National Childbirth Trust (NCT) was illegally exposing customers' credit card

details over the Internet. First, the NCT was hit by fines from the credit card companies concerned. Second, the Trust was forced to either upgrade its security measures to those expected of a larger retailer, or relocate its credit-card processing services to a specialist provider. The breach was not the fault of the NCT itself, but of a third-party e-commerce vendor who has since gone into administration.

Compliance with basic security principles is now mandatory for anyone doing business with the payment card industry. The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide standard designed by the major players in the payment card industry as a means of establishing a baseline level of security for all e-commerce businesses. While smaller enterprises are allowed to assess themselves on a six-monthly basis, failure to comply can result in the loss of the ability to process credit card payments, or in fines in the case of a security breach. As a result, it's in your best interests, should you be involved in selling products or services online, to ensure that you comply.

Typical E-Commerce Attack



The principle requirements are that you:

- Install and maintain a firewall to protect cardholder data
- Do not use vendor-supplied defaults for admin passwords or other security parameters
- Protect stored cardholder data, and encrypt any transmission across open, public networks
- Use and update anti-virus software
- Develop and maintain secure systems and applications
- Restrict data within your business on a need to know basis
- Assign a unique ID to each employee with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy addressing information security

We have covered (or will cover) many of these requirements elsewhere, and any hosting provider offering an e-commerce solution or expertise should be PCI DSS compliant themselves, and willing to help you ensure your compliance. The one aspect that may need further clarification, however, is the point about encrypted transmissions. Here we rely on SSL authentication and encryption.

As you're probably aware, SSL is the industry standard method of ensuring that communications between a client-side browser or application and your server are protected from eavesdropping or forgery, and that – through certification and authentication – your server is what it pertains to be. Even if your customers don't understand SSL themselves, there's a good chance that they'll recognise the green/yellow URL bar and padlock icon in their browser that signify its usage.

To deploy SSL you'll need a certificate. Many hosting providers now provide the option of a free shared SSL certificate for customers on their shared hosting packages, provided commerce travels through the hosting provider's shared domain. This gives small businesses and back-bedroom operations an entry-level route into e-commerce, but it doesn't reinforce the image of your company as a trusted and independent enterprise in the same way that a dedicated SSL certificate, specific to your business, does. While it's possible to obtain an SSL certificate from a third-party provider, obtaining it direct from your hosting provider can be easier. Check details like the level of encryption (128-bit or 256-bit), browser compatibility and warranty. If you're looking to set up an e-commerce application, talk to your prospective hosting provider about your needs, and check they're not trying to fob you off with a cheap but ultimately compromised product.

Finally, remember that PCI DSS is only a baseline security standard. If you and your customers demand additional layers of security, ask your hosting provider what they can provide. It takes a combination of physical, network and server security, plus careful monitoring and serious technical expertise to be a trusted hosting provider, but it also takes a capacity to listen. You owe it to your company to ensure that, whatever host you choose, they can offer all of the above.

Physical Data Security

For all the talk of hackers, worms and trojans, it's easy to forget that physical security is every bit as important as the hardware and software put in place to protect your data or your website from online attack. After all, up to 64GB of data can now be easily transferred to a single USB memory stick should someone take an unwelcome interest in your business, while servers are as vulnerable to the effects of fire, theft and flood as any desktop personal computer.

Not all providers make physical security a prime concern, and no software or hardware solution can protect against an intruder with physical access to a server, its hard drives and any password or security files stored upon it. If someone with the technical skills required gets such access, they can either steal your data straight away or create back doors that they or accomplices can exploit at a later date. And while your data might not be so valuable that anyone would want to steal it, data stolen on a server by a thief planning to do no more than sell the hardware can still end up in the wrong hands.

When just looking for a provider to support a personal or club website this isn't particularly important, but if you're trusting your provider with your business, then you should make it a priority to ask them about what physical security they provide.

Questions you might ask include:

- Are the servers in their data centres kept in a locked room?
- Who has access to those servers?
- What security measures are there to prevent unauthorised personnel from accessing the servers, or workstations connected to them on the internal company network?
- Do they have any surveillance equipment watching the servers? How many cameras do they have on each floor, and are the entrances and exits being monitored?
- Do they monitor their equipment for physical shut-downs or reboots, uncharacteristic physical connections, or suchlike?

- Are backups stored securely, and in a different room to the servers?
- Does your prospective provider offer any protection against fire or flood?
- Do they have uninterruptible power supplies or backup generators for use in the event of a power loss

While you're asking questions, find out about backup options and policies, particularly if you're looking for a shared or managed hosting or colocation plan. If they're kept in the same location as the server and not held in a secure or fireproof safe or cabinet, then the same event that wipes the data from your servers could also destroy your backup. However, if the backups are stored in an

A catastrophe in the data-centre can put servers out of action for days or weeks, and those could be days or weeks when your website, application or database is out of action and not earning its keep.

Don't underestimate the importance of these last three points. A catastrophe in the data centre can put servers out of action for days or weeks, and those could be days or weeks when your website, application or database is out of action and not earning its keep. True, many hosting providers offering professional level services will have compensation policies in place for such an eventuality, but there's no guarantee that this will make up for work or business lost due to downtime. Similarly, server time lost through a power failure can – with the worst timing – hit your business harder than you might expect.

Generally speaking, the data centres in which a hosting provider holds its servers are divided into four 'tiers', each tier defined by factors such as the number of independent power supplies feeding the racks, the height of any raised floors (for airflow and cable management), the cooling systems, the presence of backup batteries or generators and the guaranteed availability of the servers being stored. A Tier 1 data centre offers only the most basic facilities you might expect of a server room, while a Tier 4 offers state-of-the-art facilities complete with the latest biometric security measures. High-end, corporate level providers will normally operate a Tier 2 or Tier 3 equivalent data centre, though a Tier 1 data centre is acceptable for the needs of most small and medium sizes enterprises. Finding out what level of facilities your prospective host can offer can give you an 'at a glance' idea of the level of physical security you can expect, though it's always best to drill down and find out specific details.

insecure environment, then your data is as vulnerable as it would be were the servers left without security. It's well worth your while finding out.

Physical security should never be regarded as an unnecessary feature or an optional extra. Even if you don't need 24/7 patrols or camera surveillance, you should at least know that your data is securely locked away, and that your hosting provider knows who, exactly has the key (physical or electronic). If your provider can't promise you the level of physical security your business requires, then you shouldn't trust them to provide any other forms of security either.

Zen Internet - A hosting provider you can trust

As a provider of web hosting services, broadband Internet access, colocation and business class hosting to UK businesses, Zen Internet knows how to provide rock-solid, secure hosting packages, and how to work with enterprises of all sizes to create tailored products that exactly match their needs. If you're betting your business on a provider's network and servers, you need to be sure that they're on top of every security issue and every potential threat. Let us tell you why Zen Internet is a hosting provider you can trust.

Network Security

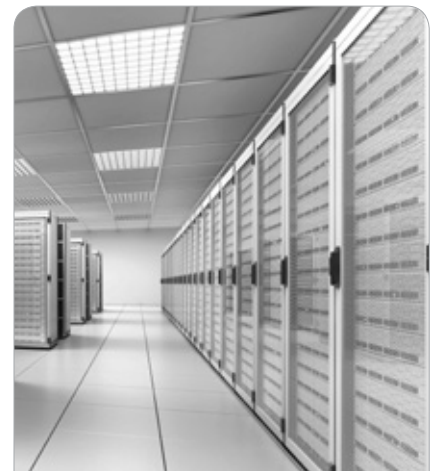
You need assurance that your websites and servers are on a network protected by enterprise-class security.

- The servers used in Zen's shared, dedicated and managed hosting packages are protected by Enterprise class firewalls, providing near wire speed firewall and intrusion detection
- Zen's network is monitored 24/7 for any sign of attack
- Zen's network is configured to make it easy to isolate compromised servers rapidly, and staff are trained to react fast in the event of abuse. Any security issue is prioritised immediately as a matter of procedure
- Zen has procedures in place to deal with any disruption, and – as a third-party security provider – the skills to combat any threat
- Zen's VPN services offer both SSL and IPSec encryption options
- Dedicated hosting packages offer a Fortigate firewall as an optional extra
- Additional security needs can be assessed and provided for on a customer by customer basis

Server Security

Your business demands servers that come configured for optimum security, and are maintained to ensure they stay that way. Access is controlled within the company to ensure your servers are accessible only on a 'need to know' basis.

- Zen provides Operating Systems hardened against online threats in line with industry standard best practice, with non-essential services removed and potential back doors firmly closed
- Zen's managed hosting packages include OS and application patching according to clear policies and schedules, with the majority of security patches applied within 24hrs of release
- Zen provides secure VPN services for remote login
- Access to managed servers only by named members of a specific support team
- Zen's managed servers are monitored 24/7
- Zen is happy to advise all customers on best security practice, and works with its customers to ensure that any vulnerabilities are dealt with promptly
- Zen provides standby hardware to cover the unlikely event of server failure
- Daily server backups maintained for a period of one month



Network Security

We assure you that your websites and servers are on a network protected by enterprise-class security

Server Security

Businesses demand servers that come configured for optimum security, and are maintained to ensure they stay that way. Access is controlled within the company to ensure servers are accessible only on a 'need to know' basis.

Overall I am incredibly pleased with the move to Zen and I feel that as we centralise our environment into Colocation within Zen the benefits of working with Zen will continue.

Stuart Morgan, IT Manager,
Explore Learning

E-Commerce Security

To comply with PCI-DSS standards, you need to know that customer and credit card data will be safe, and your customers need the peace of mind that only an SSL certificate can provide.

- Zen offers a choice of a free shared SSL certificate for small businesses (Windows Developer package only) and dedicated SSL certification for small, medium and large enterprises
- Zen's physical security standards go over and above PCI-DSS compliance
- Zen provides enterprise class firewall and anti-virus for shared and managed hosting packages, with the same available as an option on dedicated packages
- Our company continually monitors and improves its security policies in order to maintain high levels of security in an increasingly hostile online world

Physical Data Security

You need to know that your websites and your business data are running on servers where physical access is controlled, security is tight and fire and power failure won't cause you any problems.

- Zen has its own purpose built data centre, backed by 24/7 CCTV security, on-site security and the server rooms and corridors accessible only via keycards, monitored by a central management system
- Uninterruptible Power Supplies (UPS), dual utility feeds and an onsite backup diesel generator ensure a constant, 100% available power supply
- High availability heating, ventilation and air conditioning systems guarantee 99.97% uptime
- VESDA air samplers and Inergen gaseous fire suppression systems protect equipment from fire damage
- Physical access is provided under tight controls, with other customers visiting the server rooms only with the accompaniment of a Zen engineer
- Zen also manages data centre capacity at three other PoPs (Points of Presence) across the UK



E-commerce Security

To comply with PCI-DSS standard, you need to know that customer and credit card data will be safe, and your customers need the peace of mind that only an SSL certificate can provide.

Physical Data Security

We ensure that your websites and your business data are running on servers where physical access is controlled, security is tight and fire and power won't cause you any problems.

Zen's consultative approach recommended a hosting solution that met our technical and commercial requirements both now and in the immediate future. Their support team has proved to be a valuable resource in helping us migrate to the new platform with ease.

Nobin Rashid,
Hallmark

Putting it all together

While there's scope for human error, either in software development, network management or server administration, no hosting provider can guarantee perfect security. What they can guarantee is that they take a holistic approach to security, and that they have the systems and processes in place to keep your servers and data secure. Security isn't just about having the right software and the right hardware and keeping it all up to date; it's about understanding that any network or data-centre is only as secure as its least secure component, and so knowing that it all has to be locked down. In the end, budget is always an issue, and you can't expect Fort Knox for bargain basement money, but if your prospective provider can't provide the security you need across their network, their servers and their physical premises, your choice is simple. Don't sign on the dotted line. Take your business elsewhere, and find a hosting provider you can trust.

Choosing a hosting provider isn't just a matter of balancing price against bandwidth, performance and capacity – it's a question of choosing a hosting provider you can trust. We have 15 years experience in the industry and a deep understanding of what UK businesses need, and we're happy to advise and find the right hosting package for you.

To learn more:

Website: www.zen.co.uk/hosting

Tel: 0845 058 9104

Email: sales@zen.co.uk



Zen Internet

Sandbrook Park, Sandbrook Way, Rochdale OL11 1RY

Tel: 0845 058 9080 Fax: 0845 058 9140 Email: partner@zen.co.uk Web: www.zen.co.uk/partner
© 2012 Zen Internet Ltd. The information contained herein is subject to change without notice. Zen Internet shall not be liable for technical or editorial errors or omissions contained herein. All Rights Reserved v12-02.11.12