iPrimitus
CONSULTANCY SERVICES

INFORMATION SECURITY SERVICES

Network security strategic consulting

If your network isn't correctly configured, it could be vulnerable to hackers, identity thieves and other threats. That's bad news for your business ... and your customers. On top of this, the legal penalties for a security breach (that could have been prevented) are colossal, and the powers that be are typically unforgiving.

How we do it ?

At iPrimitus we audit, design and implement information security solutions in the areas of IP networking, firewalls, high availability, vulnerability assessment, security policy development, encryption, remote access, intrusion detection and prevention, content filtering, authentication, anti-virus and anti-spam.

We have secured the networks of hundreds of organizations including with complex multi-site networks, government agencies and small businesses. Our technical expertise and reputation for quality has landed us preferred partner status with the leading security product vendors.

iPrimitus believes that the best way for our customers to reduce Security threats is to develop a comprehensive security policy and implement strategies for defending their resources from external and internal threats.

Manufacturers used by iPrimitus to create solutions in this Practice Area:

- Security Policy Development
- Network Security Technology Implementation
- Network Security Testing and Assessment
- Network Security Monitoring

Vulnerability assessment Service (iVaS)

Vulnerability Assessments are a process of identifying, quantifying, and prioritizing vulnerabilities in a system. A vulnerability refers to the inability of the system to withstand the effects of a hostile environment.

VAS is a process in which the Information & Communication Technologies (ICT) infrastructure consists of computers, networks, servers, operating systems and application software which are scanned in order to identify the presence of known and unknown vulnerabilities.

As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information, product IP, customer lists etc. Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc.

Need of Vulnerability Assesment:

- A hacker has a capability to cause you huge losses and business shutdown if you don't practice infor mation security
- Data Thefts, Data Corruption, IT attacks, hacking have increased at a rate greater than 30%
- The turnover of hacking crimes surpassed drug trafficking in the USA
- Indian companies lost clientele due to lack of security practices and implementations
- The more is IT a part of your business processes, greater is the chance of IT being hacked.
- Total number of websites defaced in the year 2014 in India is 10500+ according to CERT-IN.
- Indian companies including HSBC, Wipro spectra mind, Parsec Technologies Limited, V-Angels have been victims of security breaches
- US companies invest 10-20% of their IT spending on Information Security

What could happen to you ?

- Your website will be put down and your customers won't be able to access
- Your data will be stolen and sold to competitors
- Your email accounts will be hacked/sniffed and all your communications will be recorded Your busi ness can be jammed by hanging or attacking your email server.
- All trade secrets could be leaked out.
- You may not get US, UK, Indian government and top companies as your customers as you don't follow security practices
- Your employees may use your company's infrastructure for hacking, causing legal problems to your company.
- The 6 Steps of Vulnerability Management

The 6 Steps of Vulnerability Management

- Discover and inventory assets
- Categorise and prioritise assets
- Scan for vulnerabilities
- Report, classify and rank risks
- Remediate – apply patches, fixes and workarounds
- Verify – Re-scan to confirm fixes and verify security

Benefits of VAS

- Comprehensive Testing for Applications and Networks
- Identifies the weakest link in the chain
- Eliminates false positives and prioritizes real threats
- Detection of attack paths missed through manual testing. Facilitates regular and frequent scans
- Secures against business logic flaws
- Increased IT security

Why iPrimitus ?

"iPrimitus's enterprise security assessment service covers a very wide range of assessment activities from basic security controls assessments to comprehensive enterprise assessments and threat models. Our well-refined methodologies span multiple technologies and security control areas from physical security to personnel and procedural security controls to system and application-level penetration. Each enterprise security assessment service is divided into project phases and components, customized to meet your security objectives."

Penetration Testing Services (iPenT)

A Network Penetration Test (aka, pen test) is a method of evaluating the security posture of a network system by simulating an attack from malicious outsiders who would not otherwise have authorized access to the network. Vulnerabilities are then documented and exploited in an effort to determine whether unauthorized access of malicious activity is actually possible.

The overall goal of a Network Penetration Test is to identify vulnerabilities, document them, validate them through exploitation, apply risk ratings and formally document the results in a report combined with appropriate recommendations for remediation

Our comprehensive methodology ensures that our clients' vulnerabilities are represented by their true real-world likelihood and potential impact to their business. The methodology is founded upon industry-standard frameworks, such as: OSSTMM, ISSAF, OWASP, WASC and NIST Special Publication 800 Series guidelines.

Methodology

System/service discovery consists of compiling a complete list of all accessible systems and their respective services with the ultimate goal of obtaining as much information about the assets as possible. Commonly, this includes: domain foot printing, live host detection, service enumeration, rogue system/service detection, product-specific vulnerability detection, and operating system and application fingerprinting.

With the information collected from the discovery phase, security testing transitions to identifying vulnerabilities in internal and externally facing systems and applications using automated scans and manual testing techniques.

iPrimitus begins the vulnerability identification process with a combination of commercial and open source vulnerability scanners. Automated scans are good at identifying known and common vulnerabilities, however, automated scans are not good at detecting complex security issues or validating the findings reported. For this reason, automated scans represent only a small facet of the overall security assessment with the majority of vulnerability testing focused on manual testing and verification. iPrimitus Security has adopted an industry-standard approach to assigning risk ratings to vulnerabilities. This approach is used in all our assessments and provides our clients with consistent risk ratings that take into account a number of factors ranging from: Skill Level, Motive, Ease of Exploit, Loss of Integrity, Loss of Availability to Loss in Privacy and Reputational Damage.

- Discovery/Information gathering via public websites, ARIN, job boards, domain lookup tools, etc.
- Active network scanning using networking mapping tools and manual processes.
- Enumeration of live devices searching for vulnerable services and misconfigurations.
- Exploitation of vulnerabilities to determine whether unauthorized access is possible.
- Report findings, evidence, recommendations, tools and methodology.

Our Tested & Proven Penetration Testing Process

The steps below provide a high-level outline of our proven Penetration Testing Process. This process can be augmented by Advanced Threat Modules (ATM) that include, but are not limited to, our stealth testing module, managed security service provider testing module, IDS / IPS effectiveness and tuning module, pseudo-malware module, distributed metastasis module, Social Engineering module, and many more.

Step 1: Logistics and Controls

Logistics and controls is an important yet often overlooked component of delivering quality penetration tests. The purpose of this step is to reduce the rate of false positives and false negatives by assuring proper adjustments are made to all testing modules prior to launch. This module is perpetual in that it continues to run during the entire course of testing. Its purpose is to identify any issues that may exist before testing, or to identify network or system state changes during testing.

Step 2: Advanced Reconnaissance

iPrimitus begins all penetration tests with a combination of Social and Technical reconnaissance. Social reconnaissance, not to be confused with Social Engineering, is focused on extracting information from personal websites, social networking sites like linkedin and facebook, technical forums, internet relay chat rooms, company job opportunities, documents that have been leaked or published, etc. The goal of social reconnaissance is to identify information that might assist in compromising the target. Historically this information has included source code, confidential files, passwords, troubleshooting questions about IT issues, etc.

Technical reconnaissance focuses on the discovery of hosts, service fingerprinting, configuration analysis, web server directory enumeration, the identification of administrative portals, the identification of customer portals, the identification of hidden endpoints such as cable modems or DSL lines, the use of third party services provided by hosting providers, managed security service providers, and much more. Technical reconnaissance may or may not use port scanners, web application scanners, vulnerability scanners, etc. depending on the threat and intensity levels of the service being provided.

Step 3: Analysis

Once initial social and technical reconnaissance tasks are complete, IPrimitus enters an analysis stage. During this stage all information is correlated and an attack matrix is created. The matrix identifies all potential attack vectors and organizes them by probability of successful penetration. Every identified listening port or web application component is considered to be a potential attack vector until proven otherwise.

Step 4: Real Time Dynamic Testing

Once sufficient intelligence has been gathered IPrimitus begins penetration efforts. While common tools may be used to penetrate systems with low-hanging fruit, a manually intensive research driven process is used to penetrate more complex targets. For example, bypassing a Web Application Firewall that is in line with an Intrusion Prevention System to perform successful Blind SQL Injection against an otherwise well hardened web application.

Deliverables

A comprehensive report detailing the findings, risk ratings, recommendations, methodology, tools, evidence and screenshots.

Data leakege prevention (iDLP)

Data loss prevention (DLP) is a data security technology that detects potential data breach incidents in timely manner and prevents them by monitoring data in-use (endpoints), in-motion (network traffic), and at-rest (data storage) in an organization's network.

The data in use at endpoints can be leaked via

- USB
- Emails
- Web mails
- HTTP/HTTPS
- IM
- FTP

The data in motion can be leaked via

- SMTP
- FTP
- HTTP/HTTPS

The data at rest could

- reside at wrong place
- Be accessed by wrong person
- Be owned by wrong person

A Non-Transparent Solution

Customers need more than a technology solution.

- DISCOVER:Where is their confidential data?
- MONITOR:How is it being used?
- PROTECT:How best to prevent its loss?

Benefits of Data Loss Prevention

Security executives trust IPrimitus DLP to:

- Improve visibility into their enterprise's data loss risk, deliver measurable risk reduction, and stay ahead of emerging threats and new technologies.
- Educate and protect well-meaning employees and third parties from accidentally leaking or losing confidential data.
- Prevent malicious insiders and outsiders from stealing valuable intellectual property.
- Comply with global data privacy regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and European Union Data Protection Directive.

Why iPrimitus DLP ?

Accuracy Unprecedented Detection – Machine Learning

Localization Multilingual Detection and UI Presentation

Workflow Workflow for Large Enterprises

Integration Leverage Investment in IPrimitus and Other Tools

Discover Coverage of Data Repositories

Remediation Flexible options work with your existing processes

Endpoint Endpoint Coverage and DLP for Application Control

Conclusion

- Data Loss is a huge and costly risk.
- Data Loss Prevention is about people.
- 90% of DLP is about what you do AFTER you find confidential data.
- IPrimitus DLP helps organizations protect their information against loss and theft, comply with global data privacy laws, and safeguard their reputation.
- IPrimitus is the leader in Data Loss Prevention with the most highly rated products, the most custom ers, the largest deployments and the deepest expertise.

Data encryption services (iDES)

Data is a critical asset that becomes a liability if not properly managed and secured. Protecting your data protects your business. We provide our clients with high-level data protection through selective and highly secure, column-level encryption for easy deployment, high performance and scalability.

Different points of Encryption

Endpoint Encryption
How do you protect sensitive data on endpoints while complying with various regulatory and compliance mandates?

Protect Your Customers and Your Organization
For most organizations today, the primary driver behind deploying an encryption solution is to protect customer privacy and lessen the impact of a potential data breach. In an era where cyber-attacks are growing and becoming increasingly sophisticated, it's not surprising to find that the number of data breaches has also grown exponentially.

Email Encryption
With so much customer and company information traveling by email, how do you ensure only authorized individuals can see this information both inside and outside company walls?

File,folder and cloud Encryption
Collaboration and file sharing empower your workforce, but as files multiply and travel, how do you guard against accidental or malicious exposure?

Key Features

- Up to three levels of compression, with a compression analyzer facility, so you know best whether to optimize for speed or for size
- 256-bit encryption to ensure your backups are secure
- Interactive Timeline Monitoring for easy visualization and greater control over past, present, and future activities.
- Split backups, enabling you to take advantage of multi-CPU and high-speed disk array systems to
- speed up the backup and restore process even further.
- Mirrored backups allow for creation of two or more backup files simultaneously to different disks, to minimize the probability of media errors.
- Multiple threads in the SQL Backup engine to optimize backup performance.
- Log shipping wizard, making log shipping easier
- Support for SQL Server 2005, 2008 and 2012 databases
- Built in PGP Strong - High performing, strong encryption, built with PGP Hybrid Cryptographic Optimizer (HCO) technology and leveraging AES-NI hardware optimization for even faster encryption speeds.
- Single-Sign-On – SSO means fewer passwords for users to remember.
- Key Recovery – Multiple recovery options allow organizations to determine the right solution for them to minimize potential lockouts and reduce HelpDesk calls.
- Active Directory Support – Individual and group policies and keys can be synchronized with Active Directory to help speed deployments and reduce administration burdens.
- Robust Reporting – Administrators can take advantage of out-of-the-box compliance reports or customize their own reports to help ease the burden of proof to auditors and key stakeholders.
- Heterogeneous Management – Management capabilities have been extended to include support for FIleVault2 (Apple's native OS encryption solution), as well as support for Opal compliant self-encrypting drives.

- User-Friendly – Installation and registration is completely transparent to users, while CPU utilization during initial encryption is minimized to ensure that users can continue being productive while en-
- cryption happens in the background.
- Flexible – Support multi-user deployments in both Active Directory and non-Active Directory environments.
- Collaborative – Users can access encrypted data on removable media safely even on systems without iPrimitus Endpoint Encryption installed
- Scalable – Scalable management architecture easily adapts to small and large enterprise environments.
- Stronger Protection – iPrimitus's market leading Data Loss Prevention (DLP) software integrates with removable media encryption to analyze data before it's transferred and automatically encrypt sensitive outgoing data.

Why iPrimitus Encryption?

- iPrimitus's encryption portfolio includes endpoint, file and folder and email encryption.
- Integration with iPrimitus Data Loss Prevention automatically encrypts sensitive data being moved onto removable media devices or residing in emails and files.
- Robust management features include individual and group key management, automated policy controls, and out-of-the-box, compliance-based reporting.

Encryption

To achieve maximum protection of data and maintain the best system performance, iPrimitus provides a solution that allows implementation of encryption down to the column level within the database.

- Strong Encryption – is provided with several alternative algorithms including 3DES, AES-128 and AES-256 algorithms, and with the use of CBC, IV (Initializa¬tion Vector), and CRC (Cyclic Redundancy Check) for the encrypted data.

Tokens

iPrimitus delivers the option to utilize tokens, or replacement values, to reduce the impact of compliance and to improve transparency.

Performance and Scalability

iPrimitus takes full advantage of the processing power offered by the database server and keeps machine cycles to a minimum, thus optimizing performance.

Cross Platform Support

Database Encryption is available on all leading standard Linux, UNIX or Windows environments, as well as IBM iSeries and zSeries environments, in conjunction with all major relational databases.

End poind security (iEPS)

In network security, endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connecting to the network creates a potential entry point for security threats. Endpoint security is designed to secure each endpoint on the network created by these devices.

Running a business and keeping customers happy is hard enough without also having to worry about online threats. But viruses, malware and other threats remain a reality, and they're becoming more numerous and sophisticated every year. In fact, cyber criminals are targeting small businesses to gain access to larger organizations so it's more important than ever to be sure your critical assets are protected. Online protection for your business must be powerful, but also simple, without requiring a lot of time to deploy and manage, nor require special hardware or technical expertise. And it should protect your users and machines like laptops, desktops, and servers, without slowing them down or cutting into productivity.

5 Layers of Protection:

- Network: iPrimitus's network threat protection includes Vantage technology that analyzes incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection are also included to protect against web-based attacks.
- File: Signature-based antivirus looks for and eradicates malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.
- Reputation: iPrimitus's unique Insight™ correlates tens of billions of linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, Insight™ can accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks while reducing scan overhead by up to 70%.
- Behavior: SONAR™ leverages artificial intelligence to provide zero-day protection. It effectively stops new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real-time to determine file risk.
- Repair: Power Eraser™ aggressively scans infected endpoints to locate advanced persistent threats and remove tenacious malware. Remote support enables the administrator to trigger the Power Eraser scan and remedy the infection remotely from the IPrimitus™ Endpoint Protection management console.

Key capabilities

Security

- Simple, fast, and effective endpoint
- security
- Firewall security
- Generic exploit blocking
- Web browser security

Management

- Management flexibility
- Easy setup and web-based management
- Partner management console

Reporting

- Management flexibility

Antivirus & firewall services (iAvF)

iPrimitus iAvF features both anti-virus software and firewall protection. Anti-virus protects your computer from viruses, worms, and Trojan horses in email, instant messages, and other files. The firewall enhances online security by restricting access to hackers and many Internet worms. LiveUpdate keeps your computer security up to date automatically.

What is AntiVirus Software?

Computer programs intended to Identify and Eliminate Computer Viruses. Antivirus software is a class of program that searches a hard drive and floppy disk for any known or potential viruses. Antivirus program runs in the Random Accesses Memory of a computer. Anti-virus software typically uses two different techniques to accomplish this:

- Examining files to look for known viruses by means of a virus dictionary.
- Identifying suspicious behavior from any computer program which might indicate infection.Most commercial anti-virus software uses both of these approaches, with an emphasis on the virus dictio-nary approach.

Key Features of iPrimitus Antiviruses

- Cloud-based controls in IPrimitus account let you fix, update, renew, and install IPrimitus AntiVirus over the Internet with a few simple clicks. It brings together your available IPrimitus Protection for other devices, like your Mac® computer, smartphone, or tablet, in one place.
- Delivers rapid Pulse Updates every 5 minutes to 15 minutes which run in the background for up-to-the-minute protection against the latest threats and crimeware.
- Schedules resource-intensive tasks for when you do not use your PC.
- Intelligence-driven IPrimitus Insight technology targets only those files at risk for faster, fewer, shorter scans.
- IPrimitus Protection System provides five patented layers of protection to detect and eliminate threats more quickly and accurately than other technologies.
- IPrimitus System Insight shows you how files and applications affect your computer's performance, helps to keep your computer performing its best.
- Silent Mode suspends alerts and updates to avoid interrupting or slowing games and movies.

- IPrimitus Download Intelligence 2.0 helps you to identify a downloaded file or application is dangerous before you install or run it on your computer.
- IPrimitus File Insight provides detailed information about the files in your computer including the file source (website URL) and if it can be trusted.
- Scans the email and instant messengers for suspicious links, attachments, and other tricks cybercriminals use to steal your identity and your hard-earned money.
- Vulnerability Protection guards security holes (vulnerabilities) in your operating system, applications, browsers, and browser plug-ins to prevent threats from sneaking in.
- SONAR Behavioral Protection monitors your computer for suspicious behavior to quickly detect new attacks, crimeware, and other threats.
- IPrimitus Bootable Recovery Tool to create an emergency DVD/USB that gets you back up and running when your computer is infected. You can use it even if your computer has become so infected that it won't work properly or even boot up.
- Bandwidth Management 2.0 automatically adjusts IPrimitus data usage updates when you connect to 3G networks to avoid using up your monthly data allotment or causing overage fees.
- IPrimitus Control Center gives you easy access to program settings and web-based IPrimitus services from your choice of a standard detailed view or a simplified view.
- Browser Protection proactively protects you by checking for and blocking online threats as your browser loads, to stop online threats before they can do damage.
- Power Saver Settings maximizes your laptop's battery life by putting off non-critical activities until your computer is plugged in.
- Free tech support delivers the help you need through phone, email, and chat.

What is a firewal?

A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.Acting as a barrier between a trusted network and other untrusted networks -- such as the Internet -- or less-trusted networks -- such as a retail merchant's network outside of a cardholder data environment -- a firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is; all other traffic is denied.

Key Features of iPrimitus Firewall

- Central, Powerful Management
- User and Application Control
- High Availability
- Deep Packet Inspection
- Fast and hassle-free online experience
- Blocks all Internet attacks
- Monitors in/out connections
- Manages traffic on your PC
- Secures all connections when you are online
- Web caching
- Centralized management and reporting
- Spam filtering
- URL screening