Internet Draft
draft-ietf-grip-user-02.txt
Valid for six months

T. Hansen
AT&T Laboratories

June 25, 1999

Security Checklist for Internet Service Provider (ISP) Consumers

<draft-ietf-grip-user-02.txt>

Author's version: 1.11

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This memo and its companions are discussed on the GRIP working group mailing list, grip-wg[-request]@uu.net.

Copyright Notice

Abstract

The purpose of this document is to provide a checklist for the general Internet community to use when discussing security with Internet Service Providers (ISPs). These questions can serve as a framework for discussion of security expectations with current and prospective service

providers.

1. Introduction

The purpose of this document is to provide a checklist for the general Internet community to use when discussing security with Internet Service Providers (ISPs). These questions can serve as a framework for discussion of security expectations with current and prospective service providers. Regrettably, such a discussion rarely takes place today.

This document is addressed to Internet service purchasing decision-makers (consumers). Three types of consumers are considered in this document: connectivity consumers, hosting service consumers, and co-located consumers.

Additionally, in informing ISPs of what the community will be asking of them, a further goal is to encourage ISPs to become proactive in making security not only a priority, but something to which they point with pride when selling their services. It has been argued that vendors begin to care about security only when prompted by consumers. We hope that these documents will encourage both parties to more readily express how much they care about security, and that discussion between the community and its ISPs will be increased.

Note that these are broad categories and individual consumers may not fall exactly into these categories; as such, not all questions will apply to all consumers, nor will all questions apply to all ISPs.

Companion documents, [RFCisp] and [RFCsshadd], express the general Internet community's expectations of ISPs with respect to security.

The questions have been collected together into Appendix A for easy reference.

2. Concerns Specific to Connectivity Service Consumers

2.1. Policies

2.1.1. Security Policy

** Does the ISP have a written Security Policy?

** If so, how can you receive a copy of it?

A Security Policy covers such issues as privacy, authentication, accountability, application of security patches, availability and

violations reporting. A more detailed discussion of Security Policies can be found in the Site Security Handbook [RFC2196].

2.1.2. Appropriate Use Policy

** Does the ISP have a written Acceptable Use Policy (AUP)?

** If so, how can you receive a copy of it?

When you establish a contract with your ISP to provide connectivity to the Internet, most contracts are governed by an Appropriate Use Policy (AUP). An AUP should clearly identify what you may and may not do on the various components of the system or network, including the type of traffic allowed on the networks. The AUP should be as explicit as possible to avoid ambiguity or misunderstanding.

The AUP should be reviewed each time you renew your contract. You should also expect your ISP to proactively notify you as their policies are updated.

2.1.3. Sanctions

** If there is an AUP, what sanctions will be enforced in the event of inappropriate behaviour?

An AUP should be clear in stating what sanctions will be enforced in the event of inappropriate behaviour. You should also expect your ISP to be forthcoming in announcing to the community when such sanctions are imposed.

2.1.4. Announcement of Policies

** If the AUP changes, will you be notified of changes to it, and if so, how?

You should expect your ISP to publish their security and appropriate use policies in a public place such as their web site. This way, the community can be aware of what the ISP considers appropriate and can know what actions to expect in the event of inappropriate behaviour.

2.2. Incident Handling

A Security Incident Response Team (SIRT) is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency. The Internet community's expectations of SIRTs are described in [BCP21].

2.2.1. ISPs and Security Incident Response Teams

- Does the ISP have a Security Incident Response Team (SIRT)?
  - If so,
    - What is the charter, policies and services of the team?
    - What is the escalation chain that I would follow?
    - Is it published somewhere (on the web)?
    - What is the cost of using the SIRT's different services?
  - If not,
    - What role will the ISP take in response to a security incident?
    - Is there another SIRT to whom you can turn?
- What other security resources are available from the ISP?
  - If so, at what cost?
- What other security-related services are available from the ISP?
  - If so, at what cost?

Some ISPs have Security Incident Response Teams (SIRT's). Some don't. In some ISPs, the SIRT consists of a single person; in others, a large group of people. Some ISP's provide SIRT's as an added-cost service, with the team defining as their constituency only those who specifically subscribe to (and perhaps pay for) Incident Response services.

Some of the services provided by SIRT's include: responding to attacks on the ISP's consumers, responding to attacks on other sites by consumers of the ISP, Virtual Private Network (VPN) and firewall management, and intrusion detection.

Thus it's important to determine what incident response and security resources are available to you, and define your incident response escalation chain BEFORE an incident occurs. You should find out if your

ISP has a SIRT, and if so what the charter, policies and services of that team are. (This information is best expressed using the SIRT template as shown in Appendix D of [BCP21].)

If the ISP doesn't have a SIRT, you should find out what role, if any, they WILL take in response to an incident. You should also find out if there is any other SIRT whose constituency would include yourself and to whom incidents could be reported. You may also be able to contract these services from third-party companies to perform these services on a routine or one-time basis.

2.2.2. Assistance with Inbound Security Incidents

** Will the ISP inform you of attacks against you?

** Will the ISP provide assistance to trace an attack?

** Will the ISP collect and protect evidence of the incident?

** Will the ISP guard against destruction of such evidence?

** Will the ISP guard against unintentional announcement of such evidence.

When a security incident targeting you occurs, you should expect your ISP to inform you of the attack, provide assistance to trace the attack, collect and protect evidence of the incident, and guard against its destruction or unintentional announcement.

If the event continues, you may ask the ISP to provide logging in order to further diagnose the problem, or to perform filtering of certain types of traffic.

You should ask your ISP what information they will be able to give out if another consumer is the party attacking you to determine whether or not their response is acceptable to you. Some providers may give this information freely, while others will not release the identity of the attacker without a court order.

2.2.3. Notification of Vulnerabilities and Reporting of Incidents

** What information will the ISP make available to you as security vulnerabilities are discovered in their services?

** Will they be proactive or reactive in informing you?

** How and where will that information be communicated to you?

** What information will be included in such reports?

You should expect your ISP to be proactive in notifying you of security vulnerabilities in the services they provide. In addition, as new vulnerabilities in systems and software are discovered, they should indicate whether their services are threatened by these risks.

When security incidents occur that affect components of an ISP's infrastructure, your ISP should promptly report to you:

- who is coordinating response to the incident
- the vulnerability
- how service was affected
- what is being done to respond to the incident
- whether customer data may have been compromised
- what is being done to eliminate the vulnerability
- the expected schedule for response, assuming it can be predicted
- the trouble ticket number being used to track the incident by the provider, or other suitable means of identifying the incident at a later date.

2.2.4. Contact Information

** Who should you contact via email for network security issues?

** Who should you contact via email to report inappropriate public behaviour?

** Who should you contact via email for issues relating to network infrastructure?

** Who should you contact via email for network security issues?

** ???? Anything else from the email list?

If you need to contact someone at your ISP, you should use the address SECURITY@your.isp.example for network security issues, ABUSE@your.isp.example for issues relating to inappropriate public behaviour, and NOC@your.isp.example for issues relating to network infrastructure. ([RFC2142] states that sites (including ISPs) should

maintain these mailboxes, as well as additional mailboxes that are defined for receiving queries and reports relating to specific services.) Your ISP may also have web site addresses (e.g., http://www.your.isp.example/security/) that you may use to check for expanded details on the above. You should also be able to find contact information for your ISP in Whois and in the routing registry [RFC1786].

2.2.5. After Hours

** What are the hours of operation of customer support or operations personnel?

** If reduced support is available "after hours", how can support personnel be reached in the case of a security incident?

You should recieve information for reaching customer support or operations personnel. If the ISP does not maintain 24x7 (24 hours, 7 days per week) operations (NOC, Customer Support, etc.), then some means should still be available for reaching customer support for security incidents (suspected or actual) and receiving a response in real-time.

2.2.6. Communication and Authentication

** How would your ISP communicate with you if a security incident were to occur?

** What information would be communicated with others?

You should expect your ISP to have clear policies and procedures on the sharing of information about a security incident with you, other ISPs or SIRTs, with law enforcement, and with the press and the general public. If your jurisdiction permits, you should expect to be able to conduct such communication with your ISP over a secure channel (e.g., secure web, secure Email, telephone, attended fax, etc.).

2.3. Layer 2 Security

** What measures do you take to prevent traffic taking unauthorised routes into or via your network?

** Are the networks that support your connectivity consumers and your hosting consumers segmented?

** What general measures do you take to protect your Internet facing equipment providing production services from denial of service attacks, break-ins or spoofing?

Most ISPs have firewalls of one kind or another that prevent random

packets from flowing through their network from the Internet.

Methods of segmenting networks include VLANs and non-broadcast networks. These can prevent one consumer class from affecting another consumer class.

2.4. Security Patches

** Is the ISP up-to-date in applying security patches to their software/firmware running on their production equipment?

Information about available security patches is readily available from the Center for Emergency Response Team (CERT) at http://www.cert.org. You can use telnet to connect to the port numbers of public TCP-based services (SMTP, POP, IMAP, HTTP, etc.) provided by the ISP, and check the announced version numbers for currentness and known security flaws.

2.5. Other Security Services

For the really serious consumer, additional services may be useful.

** Are port scan audits ever performed on consumer's networks and abnormal findings reported to the consumer?

** If so, how much does it cost?

** Is additional support available for auditing and securing your hosts?

** If so, how much does it cost?

** Does the ISP have a monitoring system that detects host attacks or network attacks in realtime?

** Would it be possible to test the ISP's security by mounting a deliberate attack at a mutually agreed time?

Audits run by the ISP provide tests of your own host's security. These can be useful for plugging holes on your systems.

Probes of the ISP's network can potentially be seen by them as an attack, and may lead to ramifications against you. So be careful that you do any testing of the ISP's security only with their knowledge. Freely available tools, such as ping, traceroute, SATAN and mscan, attempt a variety of probes. Most ISP's monitoring systems will pick up such probes. Useful tools of this sort can be obtained from ftp://ftp.cert.org.

2.6. References

** Will the ISP provide a list of reference customers?

If the ISP lets you speak with some reference customers, you might ask them about problems with respect to the reporting or resolution of any security incidents, as well as the security services and advice offered to them by the ISP.

3. Concerns Specific to Hosting Service Consumers

If you are hosting content on your ISP, you have additional concerns.

3.1. Acceptable Use Policy (AUP)

** What is the Acceptable Use Policy (AUP) for web content hosted by the ISP?

Generally there is a separate AUP from that used for connectivity consumers.

3.2. Physical Security

** What is the physical security of the machines used for hosting?

Machines used for hosting may be housed in unlocked cabinets. As such, there must be tight restrictions as to who may have access. Electronic access control, guards, video surveillance, etc., are all fair game. All visitors ESPECIALLY need to be escorted, as the potential for damage is much higher than in a colocation situation.

As the consumer is not generally responsible for securing the operating system or applications, there needs to be a heightened understanding of how the ISP reacts.

If you also get connectivity from the ISP (i.e., a T1), you should check to see if security for the managed site is done by a different group and check to see if the procedures for reporting and notification are much different.

Providers should do a good deal of proactive testing against, and active patching of the OS and application loads. As these loads tend to be the same from consumer to consumer, the ISP should be responsible in assuring host based security.

3.3. Backups

** How often are backups of your web content performed?

** How often are off-site backup services used?

Since the ISP is doing backups of your material, you should be aware of their frequency. Most providers also periodically send their backups to off-site locations. You may wish to provide additional back-ups of your own for the content.

3.4. Allocation of Network Capacity

** Does the ISP provide any sort of load balancing to prevent saturation of the network capacity by other customers of the ISP?

Other customers may legitimately cause a denial of service attack by hogging all of the network capacity. Providers should have standards as far as how saturated their networks may get, and should prevent this from occurring.

3.5. Spare Facilities

** What kind of spare facilities are available for use should an incident occur?

** How fast can they be deployed?

This information is useful if high availability is important to you. Cold site facilities and hot spare hardware can be important when recovering from an incident.

3.6. Managed Security Services

** Does the ISP provide a managed security service?

Many providers offer a managed security service for additional fees. Consumers are encouraged to find out what is included in the service that they are paying for, and to explore options as far as what they can do.

3.7. Content Management

** What kind of access is provided to the machine for managing your content?

** What kind of content is permitted to be hosted?

Modifying the content of your site can be performed in a multitude of ways. Some ISP's allow the content to be managed through web pages only. Some ISP's allow you to use FTP to send new content to the site. Some ISP's provide support for vendor-specific access (e.g., Microsoft FrontPage) support. Some ISP's provide a shell account for you to log in and modify the content accordingly. Some ISP's provide staging areas for you to test new content before publishing it in the normal locations. Some ISP's provide complete access to the machine being used for hosting the content, including administrative control (root access) of the machine.

Some ISP's permit only web pages to be stored. Some ISP's provide some canned CGI programs to be used. Some ISP's provide support for streaming audio or video. Some ISP's allow reviewed CGI programs to be stored. Some ISP's allow you to write and use your own CGI programs. Some ISP's provide access to other vendor-specific server facilities (e.g., Fast CGI, Server Side Scripting).

3.8. Secure Web Servers

** Does the ISP provide secure web servers (https)?

** If so, is their host certificate issued by a well-known Certificate Authority (CA)?

** Is the content provided by the secure web servers well separated from that available on their non-secure web server?

** Is the content provided by the secure web servers inaccessible by other customers?

** How would you upload content to the secure web servers?

Secure web servers provide an additional layer of security to the content. Such content must not be accessible from the non-secure web servers, nor should be accessible by other customers. The mechanisms used to upload content to the secure web server area may be different from those used to upload content to the non-secure area.

4. Concerns Specific to Co-location Consumers

If you have co-located equipment at your ISP's facility, the physical security of the installation should be given appropriate consideration. This is particularly so for co-located facilities to which people from different organisations and with different security policies have access. Many issues arise surrounding consumer access to their co-located equipment.

4.1. Acceptable Use Policy (AUP)

** What is the Acceptable Use Policy (AUP) for co-located consumers?

The AUP for co-located consumers is usually different from that used by connectivity consumers.

4.2. Physical Security

** What forms of physical security are provided for your equipment?

** What forms of supervision are provided while visiting your equipment?

Ideally you and each other consumer should have a fully enclosed locking 'cage', akin to a small room with walls and ceiling of heavy wire mesh fencing, containing the racks in which their equipment is mounted. Each consumer would be allowed access to their own cage under escort by one of the ISP's employees, by a guard, with keys or electronic access control that grant access specifically to their cage, or some combination thereof.

This assignment of separate cages is expensive in terms of space however, so many ISPs compromise by putting all co-located equipment together in a single machine room, and managing the actions of escorted consumers very closely. However this may be insufficient to prevent mishaps such as the accidental disconnection of another consumer's equipment. If a single machine room is used then the ISP should provide separate locking cabinets for each co-location consumer in preferance to an open common area. Another alternative are cabinets which can separate all of the facilities within the same cabinet, and have independent locking mechanisms for each portion of the rack.

You should expect to always be supervised while in the physical presence of any equipment that is not yours, and should not expect to be allowed to touch, photograph, or examine equipment belonging to another consumer.

4.3. Layer 1 Security

** How is co-located equipment protected electrically from other consumer's co-located equipment?

Also of importance is "layer 1" security of co-located equipment. Other consumers should not blow the same fuse that you are on by powering all their machines up at once. The ISP can control this by having

separate breakers and circuits for each consumer, or by overbuilding the power system and keeping track of the power ratings of all equipment in use.

4.4. Layer 2 Security

** How is co-located equipment protected on the network from other consumer's co-located equipment?

Also of concern is layer 2 security of co-located equipment. Your equipment should not be allowed to share a physical network segment with hosts belonging to anyone else, whether another consumer or the ISP themselves. It's common for crackers to exploit weak security or unencrypted remote logins on co-located consumer-owned equipment to take control of that equipment and put it into promiscuous listening mode on the local network segment, thereby potentially compromising the privacy and security of any other devices on that segment. The use of a switch is generally recommended for this sort of thing.

5. References

[BCP21] Brownlee, N and E. Guttman, "Expectations for Computer Security Incident Response", BCP 21, RFC 2350, June 1998.

[RFC1786] Bates, T., Gerich, E., Joncheray, L., Jouanigot, J-M., Karrenberg, D., Terpstra, M., and J. Yu, "Representation of IP Routing Policies in a Routing Registry (ripe-81++)", RFC 1786, March 1995.

[RFC2142] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, May 1997.

[RFC2196] Fraser, B., "Site Security Handbook", RFC 2196, September 1997.

6. Acknowledgements

This document is the product of input from many people and many sources. The constructive comments received from Nevil Brownlee, Randy Bush, Bill Cheswick, Barbara Y. Fraser, Randall Gellens, Erik Guttman, Larry J. Hughes Jr., Klaus-Peter Kossakowski, Michael A. Patton, Don Stikvoort, Bill Woodcock and Chris Kuivenhoven are gratefully acknowledged.

7. Security

This entire document discusses security issues.

8. Author's Address

Tony Hansen
AT&T Laboratories
Lincroft, NJ 07738
USA

Phone: +1 732 576-3207
E-Mail: tony@att.com

9. Full Copyright Statement

This document expires December 1999.

Appendix A - Collected Questions

2. Concerns Specific to Connectivity Service Consumers

2.1. Policies

2.1.1. Security Policy

** Does the ISP have a written Security Policy?

** If so, how can you receive a copy of it?

2.1.2. Appropriate Use Policy

** Does the ISP have a written Acceptable Use Policy (AUP)?

** If so, how can you receive a copy of it?

2.1.3. Sanctions

** If there is an AUP, what sanctions will be enforced in the event of inappropriate behaviour?

2.1.4. Announcement of Policies

** If the AUP changes, will you be notified of changes to it, and if so, how?

2.2. Incident Handling

2.2.1. ISPs and Security Incident Response Teams

** Does the ISP have a Security Incident Response Team (SIRT)?

** If so,

** What is the charter, policies and services of the team?

** What is the escalation chain that I would follow?

** Is it published somewhere (on the web)?

** What is the cost of using the SIRT's different services?

** If not,

- ** What role will the ISP take in response to a security incident?
- ** Is there another SIRT to whom you can turn?

** What other security resources are available from the ISP?

- ** If so, at what cost?

** What other security-related services are available from the ISP?

- ** If so, at what cost?

2.2.2. Assistance with Inbound Security Incidents

** Will the ISP inform you of attacks against you?

** Will the ISP provide assistance to trace an attack?

** Will the ISP collect and protect evidence of the incident?

** Will the ISP guard against destruction of such evidence?

** Will the ISP guard against unintentional announcement of such evidence.

2.2.3. Notification of Vulnerabilities and Reporting of Incidents

** What information will the ISP make available to you as security vulnerabilities are discovered in their services?

** Will they be proactive or reactive in informing you?

** How and where will that information be communicated to you?

** What information will be included in such reports?

2.2.4. Contact Information

** Who should you contact via email for network security issues?

** Who should you contact via email to report inappropriate public behaviour?

** Who should you contact via email for issues relating to network infrastructure?

** Who should you contact via email for network security issues?

** ???? Anything else from the email list?

2.2.5. After Hours

** What are the hours of operation of customer support or operations personnel?

** If reduced support is available "after hours", how can support personnel be reached in the case of a security incident?

2.2.6. Communication and Authentication

** How would your ISP communicate with you if a security incident were to occur?

** What information would be communicated with others?

2.3. Layer 2 Security

** What measures do you take to prevent traffic taking unauthorised routes into or via your network?

** Are the networks that support your connectivity consumers and your hosting consumers segmented?

** What general measures do you take to protect your Internet facing equipment providing production services from denial of service attacks, break-ins or spoofing?

2.4. Security Patches

** Is the ISP up-to-date in applying security patches to their software/firmware running on their production equipment?

2.5. Other Security Services

** Are port scan audits ever performed on consumer's networks and abnormal findings reported to the consumer?

** If so, how much does it cost?

** Is additional support available for auditing and securing your hosts?

** If so, how much does it cost?

** Does the ISP have a monitoring system that detects host attacks or network attacks in realtime?

** Would it be possible to test the ISP's security by mounting a deliberate attack at a mutually agreed time?

2.6. References

** Will the ISP provide a list of reference customers?

3. Concerns Specific to Hosting Service Consumers

3.1. Acceptable Use Policy (AUP)

** What is the Acceptable Use Policy (AUP) for web content hosted by the ISP?

3.2. Physical Security

** What is the physical security of the machines used for hosting?

3.3. Backups

** How often are backups of your web content performed?

** How often are off-site backup services used?

3.4. Allocation of Network Capacity

** Does the ISP provide any sort of load balancing to prevent saturation of the network capacity by other customers of the ISP?

3.5. Spare Facilities

** What kind of spare facilities are available for use should an incident occur?

** How fast can they be deployed?

3.6. Managed Security Services

** Does the ISP provide a managed security service?

3.7. Content Management

** What kind of access is provided to the machine for managing

your content?

** What kind of content is permitted to be hosted?

3.8. Secure Web Servers

** Does the ISP provide secure web servers (https)?

** If so, is their host certificate issued by a well-known Certificate Authority (CA)?

** Is the content provided by the secure web servers well separated from that available on their non-secure web server?

** Is the content provided by the secure web servers inaccessible by other customers?

** How would you upload content to the secure web servers?

4. Concerns Specific to Co-location Consumers

4.1. Acceptable Use Policy (AUP)

** What is the Acceptable Use Policy (AUP) for co-located consumers?

4.2. Physical Security

** What forms of physical security are provided for your equipment?

** What forms of supervision are provided while visiting your equipment?

4.3. Layer 1 Security

** How is co-located equipment protected electrically from other consumer's co-located equipment?

4.4. Layer 2 Security

** How is co-located equipment protected on the network from other consumer's co-located equipment?