Avira White Paper

Virus Defense Process

www.avira.com

CONTENTS:

1. PRELIMINARY CONSIDERATION

Networked world. Our world is networked. The Internet and email render geographic distances almost meaningless. This benefits both companies and private individuals: information is available worldwide, workflows become faster and more economical, and companies can be present worldwide with little effort and thus expand rapidly. Global competition and international collaborations can help reduce costs and increase quality.

Threatened network. However, our networked world is also vulnerable. Disruptions on the Internet have a worldwide impact. Malicious software such as a computer virus can very quickly spread over continental borders. Data records can be destroyed in the briefest period of time, software and hardware damaged irreparably, and companies' survival threatened.

New threats. These threats are not limited to "classic" viruses that attach themselves to programs, spread and cause damage in the file system.
New and more dangerous types of virus are emerging every day: Trojans are sent via emails or smuggled into the system through exploits and have now become the main cause of damage. "Worms" can multiply quickly, without depending on a host program. Polymorphic viruses alter their appearances in many ways, making it almost impossible to detect the mutations using conventional methods. Spyware intercepts sensitive information before it is encrypted for transmission, thus circumventing installed security measures. Personal data such as addresses, credit card numbers, passwords, etc., is therefore unprotected, facilitating abuse. Adware usually records anonymized data for marketing purposes. For example, that includes information about the user's browsing habits or the software features he or she uses most often. In many cases, adware is also bundled with other free download programs. The user is often not informed that adware is present in his or her system.

Prevention. A conscientious system administrator will therefore make data security a critical focus. Clear assignment of access rights, regular data backups, and the use of up-to-date and reliable virus protection software can help avoid the majority of the threats, like viruses, lurking on the Internet. However, each new software installation and each extension of a network can present a potential point of vulnerability for malicious software. Reliable virus protection, effective combating of viruses, and minimizing of potential damage therefore require a clearly defined process involving both the virus protection software developer and its customer. In this context, we are presenting our process for combating newly detected viruses.

2. THE STEP-BY-STEP PROCESS AT AVIRA – OPTIMAL VIRUS PROTECTION

We work with our customers to effectively combat viruses and ensure the quickest possible repair of the infected system (see Process overview – page 7). We achieve the necessary process security by automating flows wherever possible and through clearly defined steps at any point in time. In this section, we describe our role in relation to combating viruses.

Discover viruses before they spread

On the Internet front. To detect new viruses, wherever possible and before they reach the customer, our experts from the Avira Protection Lab are constantly active on the Internet - 7 days a week, 24 hours a day - and monitor a wide range of topical websites and forums.

Synergies. We engage in continuous exchanges with other professional virus protection providers and software manufacturers. Collaborations with international test institutes (AV-Test, AV-Comparatives, Virus Bulletin, and EICAR) also guarantee that our information is always up to date. Online monitoring tools allow us to detect typical mass emails with potentially dangerous viruses at an early stage and intercept them for analysis.

The customer as an informer. Of course, our customers can also send us files potentially infected by unknown viruses at any time. The detection of a new virus then triggers the actual process for combating the virus and repairing the infected system.

Step 1: Detect new virus

Avira uses cutting-edge processes in relation to combating viruses and IT security to detect any new, unknown viruses at an early stage.

Heuristic processes. In heuristic virus detection, the virus protection software does not look for the detection pattern of a program classified as malicious. In-

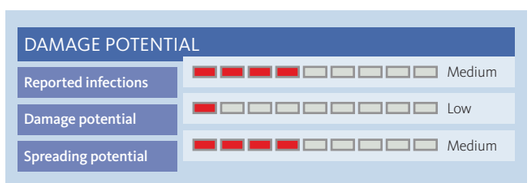
stead, it examines the actual program code in relation to its behavior when executing the program. Programs with behavioral patterns typical of viruses (for example, accessing the boot sector, integrated replication mechanisms, and data destruction routines) are classified as "suspicious" and immediately examined.

Email attachments. Frequently occurring attachments of the same kind in emails are often an indication of Trojans or worms, which spread on a massive scale all over the world. Our monitoring tools allow us to register the outbreak of such viruses promptly and investigate them immediately.

Avira Protection Cloud. In addition to the previously mentioned detection possibilities, the Avira Protection Cloud offers a very effective method for detecting unknown viruses as quickly as possible. "Fingerprints" are created for executable files (for example, .exe and .dll) and compared with a database. If a fingerprint is identified as a virus, the file is blocked. This technology also allows the Avira Protection Lab to react to new viruses as quickly as possible. Unknown, potentially dangerous files can be uploaded to the cloud and then classified as viruses. Thanks to the fingerprint, this file is immediately blocked in the event of queries from other products. It is then analyzed in greater depth in order to include detection of the virus family in our offline detection (VDF, engine).

Step 2: Characterize the virus (virus researching)

We characterize and classify any newly detected virus. Our experts analyze its program code. This allows us to draw conclusions about the virus's behavior, the damage it causes, its spreading mechanisms, and in short, the actual threat it poses.



Example of a rough classification of a virus

Step 3: Actively seek out information about the virus threat

Active virus alarm. Customers with special support contracts receive notifications by SMS, telephone, fax, or email at any time, day, or night. In parallel to this information, we train our support staff so they can properly advise our customers based on the latest information.

Step 4: Update Avira software in the test system

Remedy. The next step involves developing a remedy for the new virus. To do this, our programmers infect our virus test systems with the new virus. They determine the search string which makes the virus detectable and use this to update the virus detection pattern file.
Virus protection software that causes false alarms can be costly.Virus protection software that causes false alarms can be costly. So, Avira also uses a new process based on artificial intelligence (AI) to classify search strings for possible false alarms.
Repair routines are implemented in the Avira software depending on the nature and effect of the virus. These repair routines support our customers with cleanups of infected data and restorations of system integrity.

Quality assurance. Although speed is important when developing up-to-date virus protection software, the Avira update is then thoroughly tested in our test system. The most important points include:

- Does Avira detect the new virus reliably?
- Does Avira remove the new virus reliably?
- Does Avira restore the original condition of infected files during the repair?
- Does Avira avoid false alarms?

Only after all tests have been passed, do we take the software to the next step.

Step 5: Generate Avira update in the test system

Update files. In this step, we make sure that the update of the new software will proceed smoothly for the customer. We send the new Avira files to our release system, which automatically generates the program packages for the update and the update information files for a correct download.

Quality assurance. This step is once again followed by quality assurance: using our "fake server," we check to ensure that the automatic update of our software will run smoothly for the customer.

Step 6: Release Avira update

Only on completion of these tests do we release the Avira update and make it available on our web server.

"Magic triangle." Some time may pass between the discovery of the new virus and the availability of the Avira update. Our focus, however, is developing products as quickly as possible while at the same time ensuring they meet our company's high quality standards. The aim is to achieve the "magic triangle" of quality management (highest possible quality within the shortest possible time, in line with a reasonable price policy).

Step 7: Actively inform customers of the Avira update

As soon as the Avira update is available, we inform customers in our newsletter and, of course, on our website. The customer can then update his or her Avira software using the automatic update service to bring the virus protection back up to date.

3. THE STEP-BY-STEP PROCESS FOR THE CUSTOMER – SYSTEM INTEGRITY

Protect systems using Avira software

The software provides our customers' systems with comprehensive protection during operation from the many threats posed by viruses, worms, Trojans, and other undesirable programs. Our customers can also send suspicious files and potentially dangerous software to our support operation and thus contribute to the detection of new viruses.Our customers can also send suspicious files and potentially dangerous software to our support operation and thus contribute to the detection of new viruses.

Step 1: Initiate immediate measures

Information from Avira. In the event of a threat to their systems from new viruses, we warn our customers through our website; and in the case of support contracts, also by SMS, telephone, fax, or email. This allows our customers to implement immediate protective measures pending the software update.
Depending on the potential threat posed by the virus, these protective measures can range from increased attention to certain types of email attachments through to deactivating the email service or complete temporary disconnection from the network.

Disconnection from the network. To stop a virus from spreading any further, disconnection from the network can be taken as an additional step. We recommend disconnecting the network cable from the PC in this case.

Repair. In order to guarantee safe removal, all Avira modules should be brought up to date. In the case of a standard configuration, this is carried out using the automatic product update. If the computer needs to be disconnected from the network, an offline update can be imported instead. The Fusebundle Generator is required

for this. It can be downloaded from the Avira website (http://www.avira.com/en/downloads#tools). The Fusebundle Generator initially downloads an all-in-one update to a non-infected system. The resulting archive can then be installed on the compromised system using the Avira GUI. A complete system scan should be run on successful completion of the update. After the system scan, Avira offers the option of repairing the identified infections and placing the files in quarantine. If the system scan was not successful, the PC can be repaired using a live system. Avira offers the Rescue System for this.

Step 2: Inform your own company – Trigger virus alarm

Although timely circulation of a virus threat within a company cannot entirely eliminate the risk of damage, it can significantly reduce it. Many of the spectacular virus "accidents" of recent years could have been greatly alleviated if the wide circle of users had been better informed of the threats and methods for prevention.

Forwarding information. We pass on our information about new viruses to our customers as quickly as possible. In the event of a virus alarm, a conscientious system administrator will forward this information in an appropriate format to affected users as quickly as possible.

Increased caution. Users should then be even more vigilant in terms of looking out for and proceeding cautiously with suspicious files. This is a precaution that should apply as a basic rule for all employees of modern companies.

Step 3: Carry out software update

We inform our customers as soon as the software has been updated and can be used effectively against the new virus. The customer is automatically brought up to date using the implemented auto-update function.

Step 4: Remove the virus

The up-to-date software can now be used to check the system for infection. Files infected with the new virus can be isolated using the usual method or repair. Whether a scan of certain or even all files should also be performed depends to a great extent on the nature of the virus and the system. The administrator is responsible for deciding on the specific procedure, calling on our advice as required.

Step 5: Establish system integrity

The objective of this step is to restore the system's data pool to the status prior to the virus infection. The extent of the task will, of course, depend on the damage caused by the virus infection.

Remedying damage. If a system scan returns no findings, no special measures are required. Otherwise, depending on the severity of the infection, the procedure can range from a system scan and automatic repair to importing of a data backup.

Rebooting services. Following restoration of the data pool, any deactivated services (e.g. email service) can be restarted and users informed, if necessary.

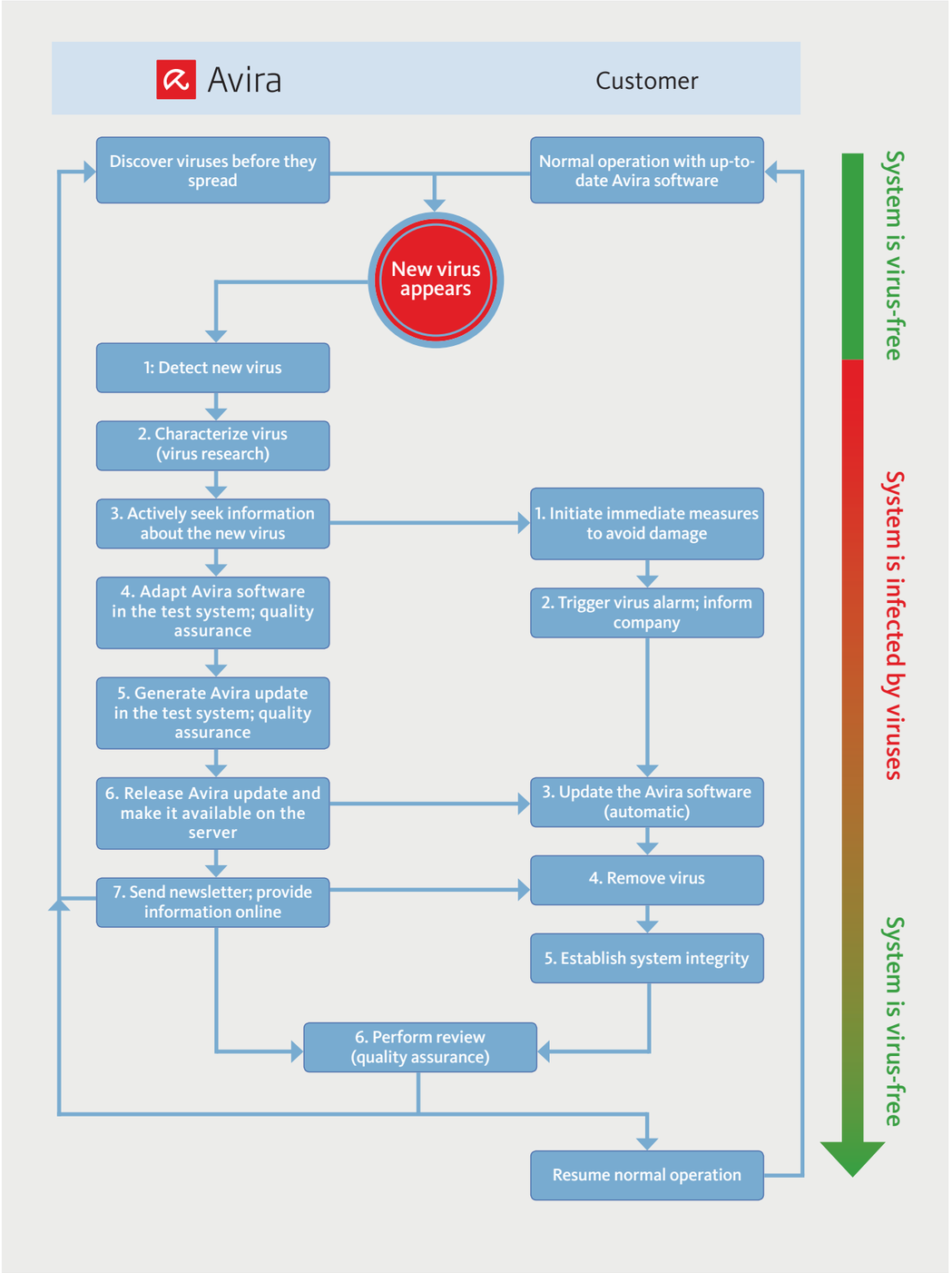
Step 6: Perform virus infection review

Critical questions. The process is concluded with an important quality assurance step: a critical review of the company's current procedure for virus infections and combating viruses. The questions are relatively simple: What went well? What went wrong? How can we avoid mistakes next time? What can we improve next time?

Lessons for the future. In some cases, finding answers to these questions may prove far more difficult. This is where we become involved, in our role as professional virus protection providers. We contribute our extensive experience to the review and provide recommendations for possible improvements in the customer's virus protection processes.

Feedback to Avira. Conversely, we also accept feedback from our customers. We address any criticisms or suggestions in order to support our customers even better, faster, and more effectively in the future, in this battle against online threats.

4. PROCESS OVERVIEW



5. CONCLUSION

The many, varied threats from malicious software against our highly networked world make comprehensive virus protection even more important than ever. We rely on two key pillars to effectively combat viruses:

- The high quality of our software
- Professional cooperation with our customers

Avira: virus protection software at the highest level

Made in Germany. With our software there are no sacrifices in terms of quality. We develop German-engineered products, across our entire portfolio, independently of external suppliers. We perform virus research and analysis in our own Avira Protection Labs, allowing us to react rapidly and flexibly to any new developments. Shift work and Avira Protection Labs in different time zones also guarantee 24-hour coverage.

Cutting-edge technologies. We continuously apply and enhance the latest software development and security technology trends. Heuristic methods for detecting unknown viruses and AI processes for virus classification are included. We create and modify our products according to strict internal guidelines over the course of clearly defined development processes.

Certificates. We have been able to demonstrate the quality of our products in a number of tests, most recently through certificates issued by the BSI (Federal Office for Information Security, http://www.bsi.de), Stiftung Warentest (http://www.test.de/), the test labs of AV-Comparatives (http://www.av-comparatives.org/de/), AV-Test (http://www.av-test.org/), and Virus Bulletin (http://www.virusbtn.com/index). We have also cooperated with the CSI (Computer Security Institute, http://www.gocsi.com) and the OPSEC (Open Platform for Security, http://www.opsec.com). For further information, please visit our website (http://www.avira.com).

Our customers and us: Working together to combat online threats

Support at all times. We enhance the high quality of our software with professional customer support. Our English-speaking customers in particular benefit from our customer orientation and English-language support, around the clock and 7 days a week if necessary. Our approach is underpinned by flexible responses to our customers' requirements.

Interfaces In this article, we have defined and explained the interfaces between us and our customers in the process for combating viruses. This approach allows us to work together to achieve maximum protection from online threats and address new and present challenges every day.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang | Germany
Phone: +49 (0) 7542-500 0
Fax: +49 7542-500 3000
www.avira.com