Eight Emergency Preparedness Testing Scenarios

Malware - Unknown Media - Physical Security
Power Outage - Ransomware - Website Hack

SBS
CyberSecurity

www.sbscyber.com

Malware: Attack of the Popup Messages

Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don't have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

A remote user has just called you, the information security officer, complaining about annoying popup messages. At first you figure that they must be doing some online shopping on an annoying website that is trying to get them to make additional purchases. Even though your users should not be shopping while on the clock, you know it sometimes happens. However, the user then tells you that the messages say "WARNING! Your Computer May be Infected" and list an 855 number to call for emergency tech support.

Discussion

- What is the most likely cause of the issue?
- What controls, if any, should have prevented this issue?
- Is there an existing policy or procedure to guide you in resolving this issue?
- What needs to be done?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?
- What additional types of user education should be integrated into security awareness and training programs?

Malware: Attack of the Popup Messages

Page 2

Inject #1

You remote into the user's computer to take a closer look, close all the browser windows and restart their computer. The issue appears to be resolved but you would like to prevent it from happening again. You try looking at the user's browser history to see what websites they have visited recently but it is empty. The user then mentions that they have a list of 12 real estate websites they visit every day and they show you where they are bookmarked.

Discussion

- How does this new information change your response to the issue?
- What is your plan for checking the bookmarked websites to see if they are infected?
- How will you know if the computer is infected with malware or if the popup messages were just a scare tactic?

Inject #2

You take a screenshot of the bookmarks so you can look at the websites in a controlled environment. You view each website and you find that one of the websites is infected with malware that clears the browsing history and caused the popup messages that the user was seeing.

Discussion

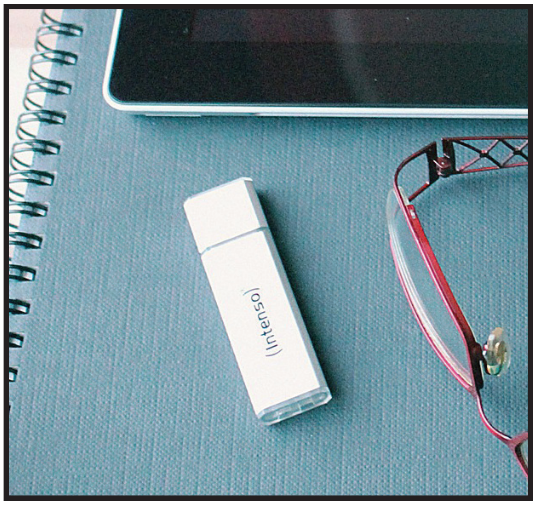
- What, if anything needs to be done to the user's computer?
- Do you need to do anything with the systems that are connected to the user's computer via mapped drives or other type of shares?
- Does this user need additional training?
- Does this incident need to be reported to anyone or formally documented in an incident report?
- Are there escalation procedures to notify management or board?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Unknown Media: You Won’t Believe What I Found

Page 1



Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don’t have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

An employee thought they made a great find in the parking lot when they picked up a USB drive labeled “Employee Bonuses”. You learned of the USB drive when the Human Resources Manager brought it to you. They explained that the employee who found the USB drive turned it in and said they had not attempted to look at the contents. The HR Manager is fairly sure the USB drive did not come from our office but would like you to see what it contains. They have heard of malicious software being distributed in this way and that’s why they brought it to you instead of looking at the contents on their own.

Discussion

- What needs to be done?
- What might the USB drive contain?
- What controls, if any, are in place to prevent the contents of the USB drive from harming your organization?
- How can you determine if an employee attempted to open the USB drive?
- What are safe methods to review the content of the USB drive?

Unknown Media: You Won’t Believe What I Found

Page 2

Discussion, continued

- Is there an existing policy or procedure to guide you through the process of looking at the contents of the USB drive?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?
- What additional types of user education should be integrated into security awareness and training programs?

Inject #1

On an isolated computer that is not connected to your network you check the USB drive and discover it contains a keylogger program that is set to auto start when the USB is put into a computer. The program then attempts to send the recorded keystrokes to a malicious server on the Internet.

Discussion

- How does this new information change your response to the issue?
- How might you block information from reaching this server if other employees are targeted.
- How can you share this information with other institutions or law enforcement?

Inject #2

The user who found the USB drive in the parking lot has confessed to trying to look at the contents of the USB drive before turning it into the HR Manager. They said there didn’t appear to be any files on the USB drive when they looked at it but their computer has not been working right since the USB drive was inserted into the computer. Everything seems to be running a little slow, it sometimes takes a second or two for the letters and words to appear on the screen after they type them, and they have seen a couple of brief popup messages that say something about connecting to a server. And, by the way, when they couldn’t see any files on the USB drive when they put it in his computer, they tried a couple of other computers in his department.

Discussion

- How does this new information change your response to the issue?
- Will you be able to tell what information, if any, has been sent outside of your network?
- Does any communication need to be sent to users, management or customers?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Physical Security: Who Left the Server Room Door Open

Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don't have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

It's Monday morning and the first person to arrive at your data center finds the server room door propped open. This is not only unusual but alarming. As far as you can tell, all your systems are up and running and there are no obvious issues related to the server room.

Discussion

- What is the most likely cause of the issue?
- Who might have done this and how should we investigate any loss or risks?
- What controls, if any, should have prevented this issue?
- Is there an existing policy or procedure to guide you in resolving this issue?
- What needs to be done?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?
- How often is physical access for employees reviewed and who might have had access to this room?
- What additional types of user education should be integrated into security awareness and training programs?

Inject #1

A review of the security cameras that monitor the interior of the building, including the server room door, finds that the DVR hard drive has filled up and the cameras have not been recording for several weeks.

Discussion

- How does this new information change your response to the issue?
- Are there any access logs that can be analyzed?
- How often are camera recordings checked and is there a log of these?
- What settings should be changed on the DVR system to prevent this issue?

Inject #2

You notice that the box of old hard drives you keep in the server room until they are destroyed is missing. The box included a hard drive that, until last week, had been installed in the computer used by the Director of Human Resources and it almost certainly contains sensitive employee information. The hard drive was replaced because it had started to give occasional error messages but it was working fine when it was removed from the Director's computer.

Discussion

- How does this new information change your response to the issue?
- How can you determine what information was on the hard drive?
- Do you need to contact law enforcement?
- How should data sanitization procedures to change to reduce risks like this?
- Are there escalation procedures to notify management or board?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Physical Security: We Didn’t Send A Technician
Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don’t have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

A user at a remote facility calls the Help Desk to report that the network technician you sent has finished and left the building. You have no idea what they are talking about. You discover that someone showed up and said the Help Desk had sent them to take a look at a router and they were going to do something to make all the systems work faster. The user checked the person’s ID and entered the information in the Visitor Log.

Discussion

- Should the user have done anything differently before giving access to the router?
- What controls, if any, should have prevented this issue?
- How are sensitive areas secured and what employees have access to those locations? Should changes be made to reduce access?
- Is there an existing policy or procedure to guide you through your next steps?
- What needs to be done?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?
- What additional types of user education should be integrated into security awareness and training programs?

Physical Security: We Didn’t Send A Technician

Page 2

Discussion, continued

- Who is responsible for any related tasks that need to be completed?
- What additional types of user education should be integrated into security awareness and training programs?

Inject #1

You dispatch someone from your group to the remote location and they report that everything looks fine, with one exception. There is a new wireless device plugged in to the router. You have the new wireless device removed but it had been plugged in for nearly two hours and a lot of customer transactions were done during that time.

Discussion

- How does this new information change your response to the issue?
- Do you need to contact law enforcement?
- What information or data could have been accessed while the device was connected?
- Are there any log files that can be analyzed or other forensics that can be done?
- What type of technology could be used to prevent rogue access points in the future?

Inject #2

You have confirmed with management that this was not a Social Engineering test so you decide that all users at the location need to change their passwords immediately. You have contacted law enforcement but since this is not deemed an emergency it might be a while before they send someone out to investigate.

Discussion

- What communication needs to be sent to employees and management?
- What law enforcement groups should be notified and how might other organizations be warned?
- In additional to their network password, what other system or application passwords need to be changed?
- How will you know if customer data has been accessed?
- If customer data might have been accessed, what policies and procedures need to be following?
- Do you have cyber insurance and, if so, how does that change your response?
- Are there escalation procedures to notify management or board?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Power Outage: That’s Why We Have A Generator

Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don’t have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

A major winter storm has just arrived and dumped 10″ of wet heavy snow in and around your primary data center. It’s 9:00 pm and the entire city has just lost power. Since you live close to your data center, you jump in your four-wheel drive and go over to take a look. When you get there, you find the entire server room is without power.

Discussion

- What backup power sources should have kept the data center powered up?
- What controls, if any, should have prevented this issue?
- Is there an existing policy or procedure to guide you in resolving this issue?
- What needs to be done?
- Does any communication need to be sent to employees or the power company?
- Who is responsible for any related tasks that need to be completed?
- Are there escalation procedures to notify management or board?

Power Outage: That’s Why We Have A Generator

Page 2

Inject #1

It has now been 45 minutes since the power went out. It looks like the primary UPS in the server room kept things going initially but it was depleted after about 20 minutes. Your generator did not start as it should have and it is displaying a message about dangerously low coolant levels. You call the power company and they tell you they have dispatched workers but they have no idea when the power will be restored.

Discussion

- How does this new information change your response to the issue?
- How will this outage affect your users and customers, especially those located in areas not directly impacted by the storm?
- Did your UPS system let your servers down gently or might there be a potential for data loss or corruption?
- Are there resources to service your generator and how do you contact them?
- How often is the generator tested and does this procedure need to change?

Inject #2

After 2 hours the power comes back on. You stick around for a while to be sure everything comes back online and is working properly. After about 30 minutes you notice the server room is getting very warm and then you realize that neither of your cooling units appear to be working. After some investigation you determine that the power issues have caused fuses in both units to burn out.

Discussion

- How does this new information change your response to the issue?
- What will happen if you are not able to cool the server room?
- What can you do to cool the room down?
- Is there monitoring equipment that would have warned you of this if you had left before noticing?
- What vendors should be contacted and where is the contact information kept?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Ransomware: Everything Is Encrypted

Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don't have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

It's 4:55 pm on a Friday afternoon and you are about to leave when a user calls to report they are seeing messages about encrypted files and a payment of Bitcoins. Maybe it's a false alarm and since it's the end of the day you are tempted to tell the user to ignore the messages and restart their computer without clicking on anything. Instead, you remote into the user's computer, glance at the encryption messages, shut down the browser and restart the computer.

Discussion

- What is the most likely cause of the issue?
- What controls, if any, should have prevented this issue?
- Is there an existing policy or procedure to guide you in resolving this issue?
- What needs to be done?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?
- What should have been down differently them restarting the computer, does that follow the incident response procedures?

Ransomware: Everything Is Encrypted

Page 2

Inject #1

In questioning the user, you learn that they had clicked on a link in an email of unknown source several hours before calling the Help Desk. They remember seeing a popup message with another link that they clicked but doesn't recall what the message said, maybe something about scanning the computer for viruses. The user also mentions that the computer was running very slow just before they called the Help Desk.

Discussion

- How does this new information change your response to the issue?
- What concerns do you have about the amount of time that has passed since the user clicked on the link and saw the first popup message?
- If necessary, will you be able to restore the user's home drive and desktop files from a backup?
- When was the last time you tested your backup system by restoring these types of files?
- Will any data be lost due to the length of time that has passed since the last backup?
- What additional types of user education should be integrated into security awareness and training programs?

Inject #2

Since the initial Help Desk call, three more employees have called the Help Desk to report similar issues and the phone is ringing again. It looks like the ransomware was able to spread from the first user's computer and you suspect it is moving across your network via mapped drives and unsecured shared folders.

Discussion

- How does this new information change your response to the issue?
- Is there anything you can do to stop the spread across the mapped drives?
- How confident are you in your ability to back up all the data that has been encrypted?
- Does any communication need to be sent to users, management or vendors?
- Are you prepared to pay the Bitcoin ransom and, if so, do you have a policy or procedure for this issue?
- Are there escalation procedures to notify management or board?
- How could we have isolated the malware earlier in the incident process to protect the network?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Website Hack: Why Is There A Cat on Our Website

Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don't have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

To your surprise, the home page of your website has been replaced with a picture of a cat. It's a cute picture, but you are not in the cat business and you need to figure out how this happened and get your website restored as quickly as possible.

Discussion

- What is the most likely cause of the issue?
- What employees or third parties have access to manage your website
- What controls, if any, should have prevented this issue?
- Is there an existing policy or procedure to guide you in resolving this issue?
- What needs to be done?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?

Website Hack: Why Is There A Cat on Our Website

Page 2

Inject #1

After contacting someone in your Marketing Department you learn that one of the people with access to the web server was terminated earlier in the day. They believe that person may still have access to the web server, but they don't know for sure.

Discussion

- How does this new information change your response to the issue?
- Who has the ability to remove that user's account and how quickly can that be done?
- Should law enforcement be contacted?
- What are the current procedures for user access following a termination and how should they be changed?
- Are there escalation procedures to notify management or board?

Inject #2

You have contacted the website hosting company and they are working on restoring website to its previous state. They have also removed access for the employee who was fired earlier in the day. While talking to the hosting company support staff you learn that other former employees still have access to the web server. You also learn that the hosting company does not require complex passwords and your website does not use HTTPS.

Discussion

- How does this new information change your response to the issue?
- Have you been regularly auditing website user access? If not, how often should it be done and what should be the process?
- If you are able to change the password complexity, what rules should you use?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

Website Hack: I Don't Want to Go Shopping

Page 1

Ground Rules

- There are no right or wrong answers or ideas.
- To get the most out of this exercise, be open to the idea that your controls may fail.
- Use the scenario to provide context and spark creative ideas.
- If you don't have the systems, staff or facilities described in the exercise, substitute reference from your own environment or play along with the given scenario.
- The goal is to find ways to improve your organization by preparing for the unexpected.
- Leverage your existing plan to evaluate how effective it is and what additional changes are necessary.

Documentation

Encourage all employees to document the following:

1. Document the understanding and workability of response procedures.
2. Document flaws and oversight in plans, procedures and strategies.
3. Document and address areas not covered in this test, including hardware, software, personnel, data and voice communications, procedures, suppliers and forms, documentation, transportation, utilities, alternate site processing, etc.

Lessons Learned

Designate an employee to collect all documentation and develop a report on the findings of the Incident Response test. Hold a meeting with all participates and review what was discovered about the current plan, review what should be improved, and give feedback on employee involvement and education from the test.

Scenario

Several customers have called reporting that your website is now a shopping website for cheap electrical gadgets. You type your website address into your browser and you are immediately redirected to another website. You try accessing your website from your smartphone and get the same results.

Discussion

- What is the most likely cause of the issue?
- Who hosts your website and how many people know the login credentials?
- What controls, if any, should have prevented this issue?
- Is there an existing policy or procedure to guide you in resolving this issue?
- What needs to be done?
- Does any communication need to be sent to employees, management or customers?
- Who is responsible for any related tasks that need to be completed?
- Should the website be scanned periodically for vulnerabilities?

Website Hack: I Don’t Want to Go Shopping
Page 2

Inject #1

You log into your website and learn that the home page is still intact, but it has been injected with redirect code. You remove the code and that seems to resolve the issue but then you realize the redirect code has been installed on multiple pages.

Discussion

- How does this new information change your response to the issue?
- What process will you use to ensure you find and remove all the malicious code?
- Do you have a current backup of your website and do you know how to restore the website if needed?
- What additional layered controls might have prevented malware infection?
- Would a website content monitoring service have identified the changed page content earlier and alerted you to investigate the issue in a timelier manner?

Inject #2

It has now been a week since you found and removed the malicious redirect code on all your web pages. Since you were able to find all the code you did not find it necessary to restore the website from a backup. Just when things seem to back to normal, a customer calls and reports that the website is now redirecting to a shopping website again.

Discussion

- What might have caused the problem to reoccur?
- Are you prepared to do a full code review of all your website files? If so, who will do it and what will it cost?
- If you restore your website from a backup, how confident are you that the issue will not reoccur?
- What are you going to do if the problem happens again after a restore?
- Was the root cause of the problem properly identified in the earlier investigation?

Lessons Learned Follow-Up Discussion

- Did you learn anything new from this exercise?
- Do you believe your organization has done everything it can to prepare for this type of event?
- Are there any policies, procedures or controls related to this exercise that could be modified or added to reduce your risk?
- What approvals or resources are needed to improve your security poster as it relates to this tabletop exercise?
- Do you have any related questions for any of the other participants?

ADDITIONAL FREE RESOURCES

available at www.sbscyber.com.

MONTHLY HACKER HOUR

Join our interactive webinar series focused on discussing cybersecurity issues and trends.

PRODUCT DEMOS

Discover the power of our offerings with live demos scheduled each week highlighting individual products or services.

SECURITY AWARENESS TRAINING

Share our cybersecurity training tools with both your employees and your customers.

CYBER-RISK™

Go beyond the spreadsheet with an automated FFIEC cybersecurity assessment.

TRAC™ ACTION TRACKING

Remain diligent with your remediation tracking and follow up by creating security plans associated with your risk assessment.

JOIN OUR MAILING LIST

Stay current with the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity. Join our email list and be in the know!

ABOUT US

YOUR CYBERSECURITY PARTNER

SBS CyberSecurity, LLC (SBS) is a premier cybersecurity consulting and audit firm. Since 2004, SBS has been dedicated to assisting organizations with the implementation of valuable risk management programs and to mitigating cybersecurity risks. The company has provided cybersecurity solutions to organizations across the United States and abroad. SBS delivers unique, turnkey solutions tailored to each client's needs, including risk management solutions, auditing, and education. SBS CyberSecurity empowers customers to make more informed security decisions and trust the safety of their data.

FOR MORE INFORMATION VISIT WWW.SBSCYBER.COM OR CALL 605-923-8722.