Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

August 31, 2020
CS-06-2020

CONTACT US / WEB FORM SUBMISSION LOGGING

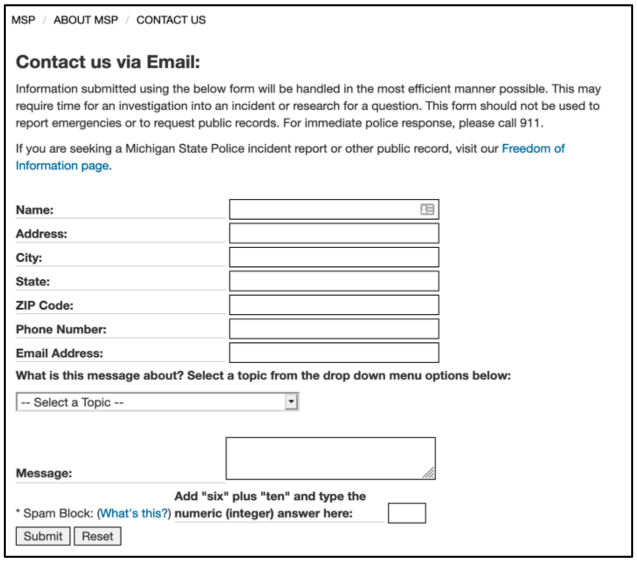
SUMMARY

To improve cybersecurity, many organizations utilize a contact us, or web form submission, instead of posting organizational structure and individual contact information online. Internet-based form submissions send an email or message to the organization, and have the appropriate staff contact the customer. These forms may have fields to request specific sets of information, or a generic text box for input. Either way, none of the data entered is typically validated to ensure its accuracy or legitimacy.

OVERVIEW

The MC3 is aware of multiple instances when online form submissions have been utilized for illegal purposes. Examples include; fake reports of self-harm, reports of harm to others, or threats of violence.

As none of the provided information on these forms are typically validated, the only way to help identify a submitter is through the user's IP address and user agent details. Capturing accurate information to identify a user can be accomplished by logging traffic to the web server or including code on the web page. Logging the web server activity generally requires an administrator be available to retrieve the information should the need arise. Embedding code on the web page can include the submitter's IP address in the data submitted to the recipient and have it immediately available. An example of HTML code to capture a submitter's IP address is: <input type="hidden" name="fpCatchIP" value="true">



MSP / ABOUT MSP / CONTACT US

Contact us via Email:

Information submitted using the below form will be handled in the most efficient manner possible. This may require time for an investigation into an incident or research for a question. This form should not be used to report emergencies or to request public records. For immediate police response, please call 911.

If you are seeking a Michigan State Police incident report or other public record, visit our Freedom of Information page.

Name:
Address:
City:
State:
ZIP Code:
Phone Number:
Email Address:
What is this message about? Select a topic from the drop down menu options below:
-- Select a Topic --

Message:

* Spam Block: (What's this?) **Add "six" plus "ten" and type the numeric (integer) answer here:**

Submit Reset

Image Source: michigan.gov/msp

Depending on network configuration, consideration should be taken to ensure the actual IP address of the user is captured, not the IP address of other internal networked equipment the data is routed through. IT staff should test and validate logging/reporting and have an idea what it takes to access this type of information when it is needed.

ANALYSIS:

Utilizing a contact us form, or generic email address, is more secure than posting organizational information and a direct contact email or phone number. Posting organizational information often leads to increased social engineering and/or targeted phishing attacks. Additionally, posting this information discloses domain details which could be used for password-spray, brute force, or social engineering attacks on listed accounts. The MC3 encourages organizations to configure their web servers or contact us web page submissions to capture or properly log a submitter's information. Organizations should have controls in place to log and identify a user in case the need arises. Consideration should be taken for the time and resources needed to access this type of information, versus including it with the information delivered to the recipient.

ADDITIONAL RESOURCES

Cyber Snapshot - Limiting Employee Information Published on Websites