MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokio, 100-8310, Japan

ZUR SOFORTIGEN VERÖFFENTLICHUNG **Nr. 3649**

Bei diesem Text handelt es sich um eine Übersetzung der offiziellen englischen Version dieser Pressemitteilung, die nur als Hilfestellung und Referenz bereitgestellt wird. Ausführliche und/oder spezifische Informationen entnehmen Sie bitte der englischen Originalversion. Im Falle von Abweichungen hat der Inhalt der englischen Originalversion Vorrang.

Kundenanfragen

Information Technology R&D Center
Mitsubishi Electric Corporation

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

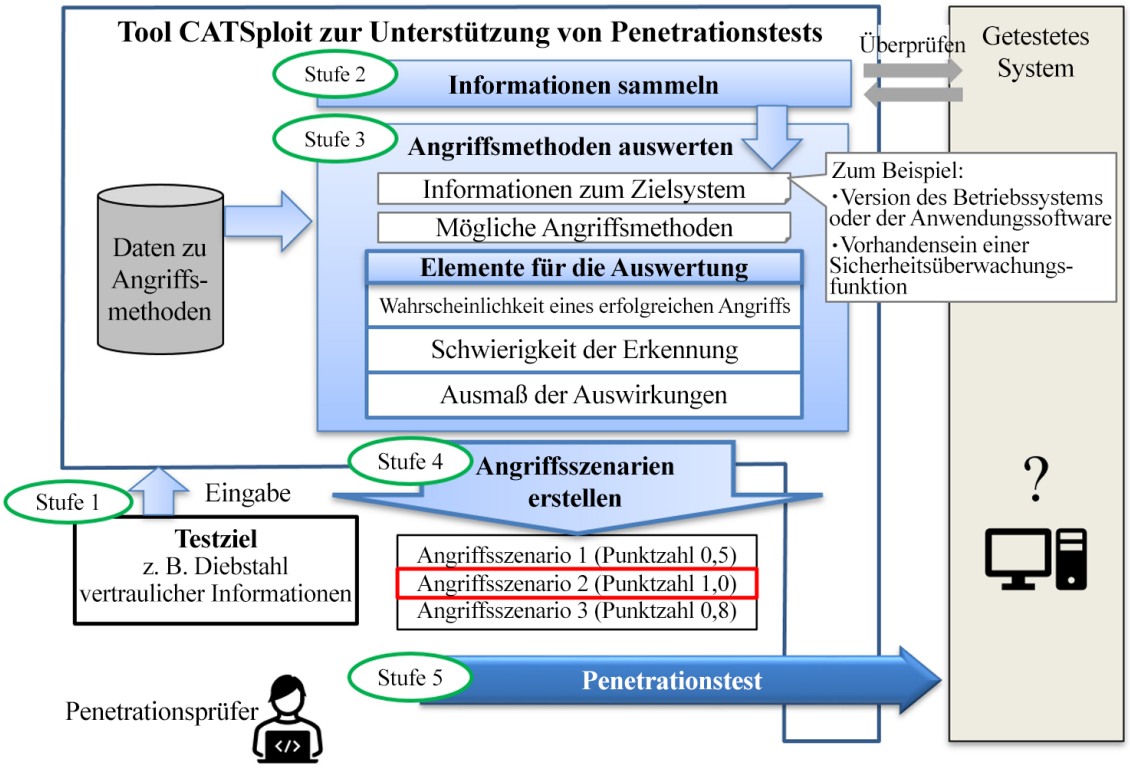
Presseanfragen

Public Relations Division
Mitsubishi Electric Corporation

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric entwickelt das weltweit erste Tool zur Unterstützung von Penetrationstests, das Angriffsszenarien aus Hacker-Perspektive generiert

Es wird erwartet, dass alle mit Netzwerken verbundenen Produkte besser vor Cyberangriffen geschützt werden können



Verwendungsbeispiel des Unterstützungs-Tools während der Penetrationstests

TOKIO, 5. Dezember 2023 – Die Mitsubishi Electric Corporation (TOKIO: 6503) gab heute bekannt, dass sie CATSploit entwickelt hat – das weltweit erste[1] Tool zur Unterstützung von Penetrationstests[2], das automatisch Angriffsszenarien auf der Grundlage der Testziele des Penetrationsprüfers generiert, z. B. Diebstahl vertraulicher Informationen. So kann die Effektivität von Testangriffen bewertet werden. Mithilfe der Angriffsszenarien und der daraus resultierenden Testergebnisse (Punktzahlen) können selbst unerfahrene Security Engineers problemlos Penetrationstests durchführen.

In den letzten Jahren wurden Steuerungssysteme für Bereiche wie Infrastruktur, Fabrikanlagen usw. zunehmend mit Netzwerken verbunden, wodurch das Risiko von Störungen wie Stromausfällen oder Ausfällen bei öffentlichen Verkehrsmitteln aufgrund von Cyberangriffen erhöht wurde. Für solche Systeme müssen dringend Sicherheitsmaßnahmen umgesetzt werden. Darüber hinaus erfordern die ISA/IEC 62443[3]-Standards, dass Sicherheitstests wie Fuzzing[4] und Penetrationstests an Systemen und Anlagen durchgeführt werden, um ihre Widerstandsfähigkeit gegenüber Cyberangriffen, einschließlich Schwachstellen aufgrund von Implementierungs- oder Konfigurationsfehlern, zu bewerten. Die Penetrationstests sind äußerst anspruchsvoll. Deshalb müssen sogenannte White-Hat-Hacker[5] involviert werden, die das zu testende System oder Produkt tatsächlich angreifen. Solche Personen, die über ein sehr hohes Maß an Fachwissen verfügen müssen, sind jedoch selten und schwer zu finden.

Mitsubishi Electric legt den Fokus auf die Faktoren, die Hacker bei der Auswahl ihrer Angriffsvektoren berücksichtigen. Das Unternehmen hat ein Tool zur Unterstützung für Penetrationstests entwickelt, das Listen möglicher Angriffsszenarien und deren Effektivität (als numerische Werte ausgedrückt) generiert.

Einzelheiten zu diesem Tool werden am 6. Dezember (11 Uhr Ortszeit) während der Veranstaltung Black Hat Europe 2023 Arsenal in London vorgestellt, die am 6. und 7. Dezember stattfindet.

Produktmerkmale

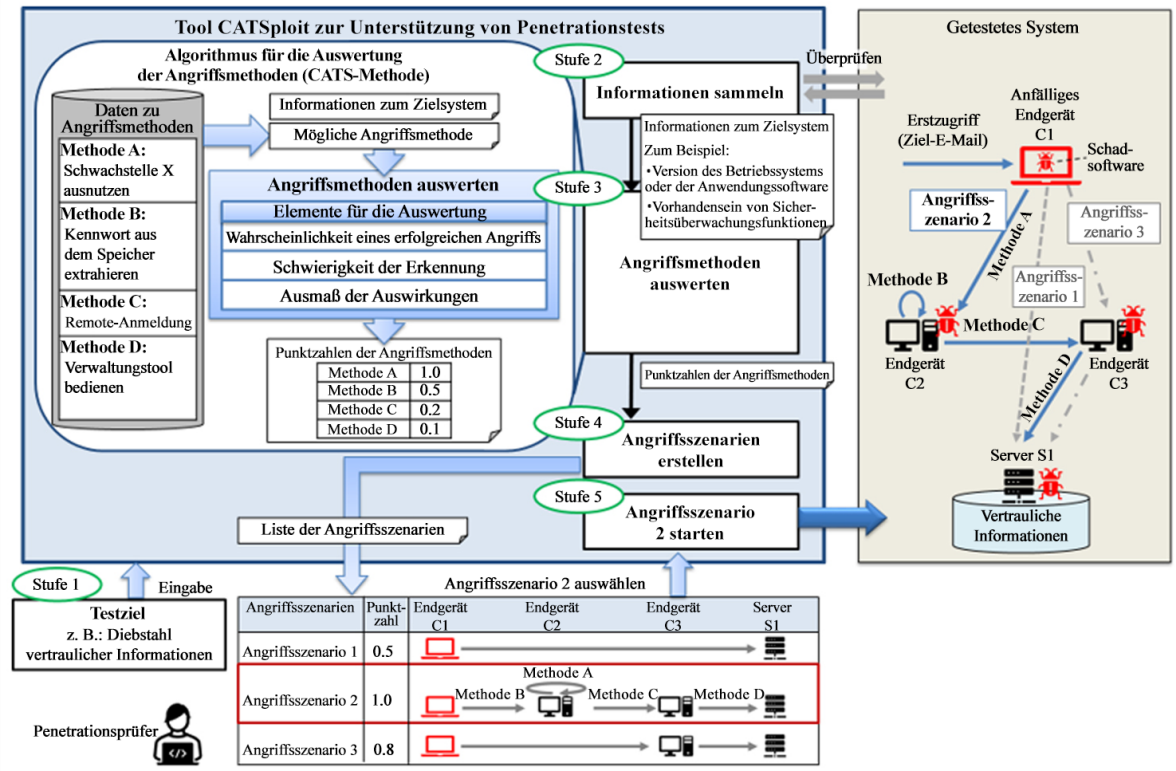
1) Generiert automatisch Angriffsszenarien aus der Perspektive von White-Hat-Hackern

- Mitsubishi Electric legt den Fokus auf Faktoren, die White-Hat-Hacker bei der Auswahl ihrer Angriffsmethoden berücksichtigen, wie die Wahrscheinlichkeit eines erfolgreichen Angriffs, die Schwierigkeit der Erkennung und das Ausmaß der Auswirkungen. Da bei bestimmten Tests Anpassungen an die Ziele vorgenommen werden, kann das System automatisch Szenarien generieren, die die Schritte aufzeigen, die zur Umsetzung eines Angriffs erforderlich sind. So können diese Ziele erreicht werden.

[1] Gemäß Forschungsergebnissen von Mitsubishi Electric vom 5. Dezember 2023
[2] Test zur Bestätigung, ob ein System oder eine Anlage durch einen tatsächlichen Angriff beeinträchtigt werden kann
[3] Sicherheitsstandards für industrielle Steuerungssysteme
[4] Eine Testmethode zur Erkennung von Softwarefehlern oder Schwachstellen durch die Eingabe ungültiger oder falscher Daten
[5] Ethisch handelnde Hacker, die fortgeschrittene Kenntnisse und Computertechnologie einsetzen, um Sicherheitsprobleme usw. zu identifizieren.

2) ***Ideale Tests bewerten die Effektivität von Angriffsszenarien aus der Perspektive eines White-Hat-Hackers***

- Die proprietäre CATS[6]-Methode von Mitsubishi Electric berechnet die Wirksamkeit jeder Angriffsmethode (ausgedrückt als Zahlenwert) aus der Perspektive eines White-Hat-Hackers. Auf Grundlage dessen wird eine Liste von Angriffsszenarien vorgeschlagen, damit das effektivste Szenario (höchste Punktzahl) ausgewählt werden kann.
- Bei der CATS-Auswertung werden nicht nur bekannte Systeminformationen wie das Betriebssystem, die Anwendungsversion und Sicherheitsüberwachungsgeräte berücksichtigt, sondern auch fehlende Systeminformationen. Dies trägt dazu bei, Angriffsszenarien aus der gleichen Perspektive wie die eines Angreifers zu realisieren.
- Durch die automatisierte Auswertung von Angriffsszenarien, die von White-Hat-Hackern wahrscheinlich verwendet werden, können weniger erfahrene Security Engineers einfach Penetrationstests durchführen.



Tool CATSploit zur Unterstützung von Penetrationstests

[6] Beurteilung der Techniken für Cyberangriffe: Proprietäre Methode von Mitsubishi Electric zur Auswertung der Effektivität von Angriffsvektoren

Zukünftige Weiterentwicklung

Um den Widerstand von Systemen und Geräten, die von Mitsubishi Electric entwickelt wurden, gegenüber Cyberangriffen weiter zu verbessern, wird das Unternehmen dieses neue Tool weiter erforschen und entwickeln, sodass es bis 2026 für die eigentlichen Sicherheitstests der Produkte des Unternehmens genutzt werden kann.

###

Über die Mitsubishi Electric Corporation

Mit über 100 Jahren Erfahrung in der Bereitstellung zuverlässiger, hochwertiger Produkte ist die Mitsubishi Electric Corporation (TOKIO: 6503) ein anerkanntes, weltweit führendes Unternehmen in der Herstellung, in der Vermarktung und im Vertrieb von Elektro- und Elektronikgeräten für die Informationsverarbeitung, Kommunikation, Raumfahrtentwicklung und Satellitenkommunikation, Unterhaltungselektronik, Industrietechnik, den Energie- und Transportsektor sowie Gebäudeanlagen. In Anlehnung an „Changes for the Better“ ist Mitsubishi Electric bestrebt, die Gesellschaft mit Technologie zu bereichern. Das Unternehmen verzeichnete konzernweit einen Umsatz von 5.003,6 Mrd. Yen (37,3 Mrd. US-Dollar*) im Geschäftsjahr zum 31. März 2023. Weitere Informationen erhalten Sie unter www.MitsubishiElectric.com.

* US-Dollarbeträge werden zu einem Wechselkurs von 134 Yen für 1 US-Dollar umgerechnet, dem ungefähren Wechselkurs an der Tokioter Devisenbörse vom 31. März 2023