Agentur der Europäischen Union
für Cybersicherheit
Agamemnonos 14,
Chalandri 15231| Attiki|
Griechenland
Tel.: +30 28 14 40 9711
E-Mail: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Erprobung der Abwehrfähigkeit des europäischen Gesundheitswesens

Im Rahmen der Strategie der Agentur der Europäischen Union für Cybersicherheit (ENISA) wurde eine Cybersicherheitsübung durchgeführt, um die Reaktion auf Angriffe auf Infrastrukturen und Dienste im Gesundheitswesen in der EU zu testen.

Um das Vertrauen der Bürgerinnen und Bürger in die ihnen zur Verfügung stehenden medizinischen Dienste und Infrastrukturen zu gewährleisten, sollten die Gesundheitsdienste jederzeit funktionieren. Wenn Gesundheitsdienste und -infrastrukturen in Europa Gegenstand eines schweren Cyberangriffs wären, wie würden wir sowohl auf nationaler als auch auf EU-Ebene reagieren und diese Reaktion koordinieren, um derartige Vorfälle einzudämmen und eine Eskalation zu verhindern?

Auf diese Frage versucht „Cyber Europe 2022“ anhand eines fiktiven Szenarios eine Antwort zu finden. Der erste Tag umfasste eine Desinformationskampagne zu manipulierten Laborergebnissen und einen Cyberangriff auf europäische Krankenhausnetzwerke. Am zweiten Tag hat sich das Szenario zu einer EU-weiten Cyberkrise ausgeweitet, bei der die unmittelbare Gefahr der Veröffentlichung personenbezogener medizinischer Daten bestand, und es wurde eine weitere Kampagne eingeleitet, mit der ein medizinisches implantierbares Produkt in Verruf gebracht werden sollte, weil es angeblich schadensanfällig sei.

Der Exekutivdirektor der Agentur der Europäischen Union für Cybersicherheit, **Juhan Lepassaar**, erklärte: *„Die Komplexität unserer Herausforderungen steht derzeit in einem proportionalen Verhältnis zur Komplexität unserer vernetzten Welt. Deshalb bin ich der festen Überzeugung, dass wir alle relevanten Informationen, die wir in der EU haben, sammeln und unser Fachwissen und unsere Kenntnisse auszutauschen müssen. Die Stärkung unserer Cyberabwehrfähigketi ist der einzige Weg, wenn wir unsere Gesundheitsdienste und -infrastrukturen und letztlich die Gesundheit aller EU-Bürgerinnen und -Bürger schützen wollen.“*

An der von der ENISA organisierten gesamteuropäischen Übung nahmen insgesamt 29 Länder der Europäischen Union und der Europäischen Freihandelsassoziation (EFTA) sowie die Organe und Einrichtungen der EU, die ENISA, das CERT-EU der Europäischen Kommission, Europol und die Europäische Arzneimittel-Agentur (EMA) teil. Mehr als 800 Cybersicherheitsexpertinnen und -experten arbeiteten in den zwei Tagen aktiv an dieser jüngsten Ausgabe von Cyber Europe mit, um die Verfügbarkeit und Integrität der Systeme zu überwachen.

Können wir die Cyberabwehrfähigkeit des Gesundheitswesens in der EU stärken?

Die Teilnehmenden an dieser komplexen Übung äußerten sich zufrieden über den Umgang mit den Vorfällen und die Reaktion auf fiktive Angriffe.

Nun müssen der Prozess und die Ergebnisse der verschiedenen Aspekte der Übungen analysiert werden, damit wir ein realistisches Verständnis möglicher Lücken oder Schwachstellen erhalten, für die gegebenenfalls Abhilfemaßnahmen erforderlich sind. Der Umgang mit solchen Angriffen erfordert unterschiedliche Kompetenz- und Prozessebenen, zu denen ein effizienter und koordinierter Informationsaustausch, der Austausch von Wissen über bestimmte Vorfälle und die Überwachung einer im Falle eines allgemeinen Angriffs eskalierenden Situation gehören. Die Rolle des CSIRT-Netzwerks auf EU-Ebene und die Standardbetriebsprozesse der CyCLONe-Gruppe müssen ebenfalls untersucht werden.

Die eingehendere Analyse wird im Maßnahmenbericht veröffentlicht werden. Die Ergebnisse werden als Grundlage für künftige Leitlinien und weitere Verbesserungen zur Stärkung der Cyberabwehrfähigkeit des Gesundheitswesens im Falle von Cyberangriffen in der EU dienen.

Über die Übungen im Rahmen von Cyber Europe

Die „Cyber-Europe“-Übungen sind Simulationen groß angelegter Cybervorfälle, die sich zu einer EU-weiten Cyberkrise ausweiten. Die Übungen bieten die Möglichkeit, komplexe Cybervorfälle zu analysieren und zu ermitteln, wie auf komplexe Situationen im Zusammenhang mit der Aufrechterhaltung des Geschäftsbetriebs und der Krisenbewältigung reagiert werden kann.

Die ENISA organisierte bereits fünf europaweite Cyberübungen in den Jahren 2010, 2012, 2014, 2016 und 2018. Die Veranstaltung findet in der Regel alle zwei Jahre statt, wobei die Ausgabe 2020 jedoch aufgrund der COVID-19-Pandemie abgesagt wurde.

Die internationale Zusammenarbeit aller teilnehmenden Organisationen gehört zu den Spielregeln dieser Übung, an der die meisten europäischen Länder teilnehmen. Es handelt sich um eine flexible Lernerfahrung: das Spektrum reicht von einem einzelnen Analysten bis hin zu einer ganzen Organisation und umfasst Opt-in- und Opt-out-Szenarien, bei denen die Teilnehmenden die Übung an ihre Bedürfnisse anpassen können.

Weitere Informationen

Cyber Europe 2022

Cyberübungen – ENISA-Thema

Cyber Europe 2018 – Maßnahmenbericht

Kontakt:

Bei Presse- und Interviewanfragen wenden Sie sich bitte an press(at)enisa.europa.eu.