Cyber Europe 2018 – Vorbereitung auf die nächste Cyberkrise

EU-Cybersicherheitsagentur ENISA organisiert internationale Cybersicherheitsübung

Stellen Sie sich folgende Situation vor: Es ist ein normaler Tag am Flughafen. Plötzlich zeigen die Check-in-Automaten einen Systemfehler an. Die Reise-Apps auf den Smartphones funktionieren nicht mehr. Die Mitarbeiter an den Check-in-Schaltern können ihre Computer nicht mehr verwenden. Die Reisenden können weder ihr Gepäck aufgeben noch die Sicherheitskontrollen passieren. Überall bilden sich lange Schlangen. Auf den Anzeigetafeln werden alle Flüge als gestrichen angezeigt. Aus unbekannten Gründen funktioniert die Gepäckausgabe nicht mehr, und über die Hälfte der Flugzeuge muss am Boden bleiben.

Berichten zufolge hat eine radikale Gruppierung durch digitale und hybride Angriffe die Steuerung der kritischen Flughafensysteme übernommen. Sie hat sich bereits zu dem Angriff bekannt und nutzt ihre Propagandakanäle, um einen Aktionsaufruf zu verbreiten und mehr Anhänger für ihre radikale Ideologie zu gewinnen.

Diesem extremen Szenario standen am 6. und 7. Juni 2018 über 900 europäische Experten für Netz- und Informationssicherheit aus 30 Ländern bei der „Cyber Europe 2018“ (CE2018) gegenüber, der bisher umfangreichsten EU-Übung zur Netz- und Informationssicherheit.

Die zweitägige Übung wurde von der ENISA an ihrem Hauptsitz in Athen (Griechenland) organisiert. Die Teilnehmer blieben entweder an ihrem gewöhnlichen Arbeitsplatz oder versammelten sich in Krisenstäben. Die ENISA steuerte die Übung über ihre Cyberübungsplattform (CEP – *Cyber Exercise Platform*). Diese stellt ein „virtuelles Universum“ für die simulierte Welt bereit, d. h. eine integrierte Umgebung, die Materialien zum Vorfall, virtuelle Nachrichtenwebsites, Kanäle der sozialen Medien, Unternehmenswebsites und Sicherheitsblogs umfasst.

Die CE2018 wurde von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) in Zusammenarbeit mit Behörden und Ämtern für Netz- und Informationssicherheit aus ganz Europa organisiert. Die Übung sollte die Fähigkeiten der europäischen Cybersicherheitskreise stärken, schwerwiegende Bedrohungen zu erkennen und zu bewältigen, und die grenzübergreifende Verbreitung von Angriffen besser zu verstehen.

Das Hauptziel der CE2018 bestand jedoch darin, Organisationen darin zu unterstützen, ihre internen Notfallpläne zur Aufrechterhaltung des Geschäftsbetriebs und die entsprechenden Krisenmanagementpläne (einschl. der Krisenkommunikation über die Medien) zu testen und gleichzeitig die Zusammenarbeit zwischen öffentlichen und privaten Einrichtungen zu fördern.

Das Szenario umfasste realitätsnahe technische und nichttechnische Cyberangriffe, die Netz- und Schadsoftwareanalyse, Forensik und Steganografie erforderlich machten. Bei der Auswahl der Vorfälle im Szenario wurde darauf geachtet, dass sie eine Krise auf sämtlichen Ebenen auslösen konnten: auf Organisationsebene ebenso wie auf lokaler, nationaler und europäischer Ebene.

Die EU-Kommissarin für digitale Wirtschaft und Gesellschaft, Mariya Gabriel, betonte: „Technologie bietet unzählige Chancen für alle Bereiche unserer Wirtschaft. Doch sie birgt auch Risiken für unsere Unternehmen und Bürger. Die Europäische Kommission und die Mitgliedstaaten müssen zusammenarbeiten und sich mit den erforderlichen Instrumenten für die Erkennung von Cyberangriffen

und den Schutz der Netze und Systeme ausrüsten. Vor diesem Hintergrund wurde die ENISA-Übung „Cyber Europe“ vor acht Jahren geschaffen. Sie hat sich zu einer wichtigen Übung zur Netz- und Informationssicherheit und zu einer Leitveranstaltung der EU entwickelt, bei der Hunderte von Cybersicherheitsexperten aus ganz Europa zusammentreffen. Wir sollten an diesen Erfolg anknüpfen und ich bin zuversichtlich, dass wir die Mechanismen der EU-weiten Zusammenarbeit weiter ausbauen können, insbesondere was die Reaktionsfähigkeit bei massiven Cyberangriffen anbelangt.“

Prof. Dr. Udo Helmbrecht, der geschäftsführende Direktor der ENISA, erklärte: „Im letzten Jahrzehnt hat die Luftfahrtbranche gewaltige technische Fortschritte gemacht. Heute nutzen wir die Vorteile von Navigations-Apps, Online-Check-in und automatischer Gepäckkontrolle. Intelligente Technologien sparen Zeit, Geld und erleichtern den Reisenden das Leben. Doch mit den Technologien entwickeln sich auch Cyberbedrohungen ständig weiter. Durch Ereignisse wie Cyber Europe 2018 stärkt unsere Agentur die Netz- und Informationssicherheit in der EU. Die moderne Antwort auf grenzüberschreitende Bedrohungen besteht in einer nahtlosen Zusammenarbeit der europäischen Länder und Organisationen. Im Auftrag der ENISA und aller Mitarbeiter möchte ich allen Beteiligten an der Cyber Europe 2018 gratulieren.“

Letztendlich konnten die Teilnehmer die Auswirkungen der Cyberangriffe rechtzeitig und effektiv eindämmen. Dies zeigt, dass der europäische Sektor für Netz- und Informationssicherheit in den letzten Jahren gereift ist und die Akteure heute viel besser vorbereitet sind. Die ENISA und die Teilnehmer werden in Kürze über das Ereignis berichten und die Maßnahmen analysieren, die zur Ermittlung verbesserungsfähiger Bereiche ergriffen wurden. Die ENISA wird zeitnah einen Abschlussbericht veröffentlichen.

Tatsachen auf einen Blick

Teilnehmende Länder: 30, Österreich, Belgien, Bulgarien, Kroatien, Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Schweden, Schweiz, Vereinigtes Königreich.

Teilnehmende Organisationen: 300,

Teilnehmeranzahl: über 900 Experten für Cybersicherheit

Anzahl der Angriffe: 23 222

Über die „Cyber Europe“-Übungen

„Cyber Europe“-Übungen sind Simulationen massiver Cyberangriffe, die sich zu einer EU-weiten Cyberkrise entwickeln. Die Übungen bieten die Gelegenheit, komplexe Cyberangriffe zu analysieren und auf komplexe Situationen zu reagieren, in denen es um die Aufrechterhaltung des Geschäftsbetriebs und Krisenbewältigung geht. Die ENISA hat bereits vier gesamteuropäische Übungen zum Thema Cybersicherheit organisiert (2010, 2012, 2014 und 2016).

Die internationale Zusammenarbeit aller teilnehmenden Organisationen gehört zu den Spielregeln dieser Übung, an der die meisten europäischen Länder teilnehmen. Sie ermöglicht eine flexible Lernerfahrung: Die Teilnehmer können die Übung auf die jeweiligen Anforderungen abstimmen, unabhängig davon, ob es sich um Einzelanalysten oder ganze Organisationen bzw. Opt-in- oder Opt-out-Szenarios handelt.