Neuer Leitfaden von ENISA: Handlungsrelevante Informationen zu Security Incident Response

Die ENISA veröffentlicht einen Good Practice-Leitfaden mit handlungsrelevanten Informationen zu Security Incident Response, der ein Bild der Herausforderungen vermitteln soll, mit denen nationale CERTs und andere Sicherheitsorganisationen konfrontiert sind, wenn sie versuchen, brauchbare Ergebnisse aus großen Datenmengen zu generieren.

Die Studie gibt einen breiten Überblick über den aktuellen Informationsaustausch im Zusammenhang mit der Generierung handlungsrelevanter Informationen, identifiziert bestehende Tools und Standards, berichtet über Best Practices und Lücken und gibt Empfehlungen zur Verbesserung..

Im Hauptteil des Berichts wird beschrieben, wie handlungsrelevante Informationen erhalten, genutzt und systematisch ausgetauscht werden. Das vorgeschlagene konzeptionelle Modell, das der Studie Struktur verleiht, stellt eine generalisierte Informationsverarbeitungspipeline mit fünf Schritten vor: Sammlung, Aufbereitung, Speicherung, Analyse und Verteilung. Anhand des Modells soll der Umfang von CERTs mit Informationen erleichtert werden, sodass der Incident Handling-Prozess optimiert wird.

Der geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, kommentierte: *„CERTs sind unsere erste Verteidigungslinie gegen Cyber-Angriffe.*
Da sie bei ihrer täglichen Arbeit immer größere Datenmengen verarbeiten müssen, besteht die Herausforderung darin, diese sinnvoll auszuwerten und handlungsrelevante Ergebnisse zu erzielen. Handlungsrelevante Informationen werden als grundlegender Baustein für Incident Response identifiziert. *Diese Studie ist der erste Versuch, einen Leitfaden zu diesem Thema für CERTs zu erstellen. Die ENISA freut sich über die Gelegenheit, weitere Arbeiten in diesem Bereich mit Berichten, Forschungen und der Weiterentwicklung von Tools zu unterstützen.“*

Die Lücken, die üblicherweise in CERT-Prozessen für den Umgang mit handlungsrelevanten Informationen zu finden sind, werden untersucht und Organisationen, die für die Verbreitung von Informationen verantwortlich sind, erhalten eine Reihe allgemeiner Empfehlungen. Insgesamt lässt sich feststellen, dass der Informationsaustausch noch nicht die nötige Reife erreicht hat und die Sharing-Umgebung weiterentwickelt werden muss, bevor die Vorteile dieses Austausches vollständig zum Tragen kommen.

Die Arbeit beinhaltet drei Fallstudien, die sich mit verschiedenen Aspekten des Umgangs mit handlungsrelevanten Informationen auf Seiten der CERTs befassen. In diesen Szenarien werden die operativen Prozesse echter CERT-Teams und die tatsächlichen Funktionen der verwendeten Tools erfasst und sodann dargelegt, wie sie verwendet werden können, um die Fähigkeiten des CERT-Teams zu verbessern, wenn es darum geht, handlungsrelevante Informationen zu erstellen, auszutauschen und zu verwenden.

Bestandsverzeichnis für den Informationsaustausch

Die Studie wird durch ein Bestandsverzeichnis mit dem Titel Standards und Tools für den Austausch und die Verarbeitung handlungsrelevanter Informationen ergänzt, das für Aktivitäten im Bereich Informationsaustausch verwendet werden kann. Es befasst sich mit den Beziehungen zwischen den verschiedenen Standards und liefert ein besseres Verständnis der zugrundeliegenden Protokolle.

Der erste Teil des Bestandsverzeichnisses enthält insgesamt 53 unterschiedliche Standards zum Informationsaustausch, eine Mischung aus Formaten, Protokollen, technischen Ansätzen und Rahmenwerken, die sehr gebräuchlich sind. Diese werden basierend auf dem Umfang des Standards in sieben Hauptkategorien eingeordnet.

Der zweite Teil des Bestandsverzeichnisses besteht aus 16 Tools und Plattformen zum Informationsaustausch, die für den Austausch und die Verarbeitung handlungsrelevanter Informationen eine wichtige Rolle spielen. Es handelt sich in erster Linie um Open-Source-Lösungen, die den CERTs zur Verfügung stehen.

Praktische Übung: Verwendung von Indikatoren, um die Verteidigungsfähigkeit zu verbessern – Handlungsrelevante Informationen

Im Rahmen des Projekts wurde ein neues praktisches Übungsszenario zu Schulungszwecken für Mitglieder von Incident Response-Teams und anderen IT-Sicherheitsfachleuten, die für Security Incident Response verantwortlich sind, erstellt.

Das Ziel dieser Übung besteht darin zu vermitteln, wie mithilfe von Collaborative Research Into Threats (CRITs)-Plattformen Gefährdungsindikatoren erstellt und eingesetzt werden können. Darüber hinaus wird dargestellt, wie CRITs eingesetzt werden können, um Beziehungen zwischen verschiedenen Elementen einer Kampagne darzustellen, wie anhand von Ereignisdaten Indikatoren erstellt, Eindämmungsmaßnahmen entwickelt und diese Maßnahmen nachverfolgt werden können. Die Übung wurde für einen strukturierteren Ansatz im Bereich Indikatorenmanagement entwickelt, was letztlich dazu führt, dass man besser für die Sicherung von Netzwerken gerüstet ist.

Die vollständigen Berichte (in englischer Sprache) sind hier abrufbar:

- Actionable Information for Security Incident Response
- Standards and tools for exchange and processing of actionable information
- Using indicators to enhance defence capabilities-Actionable information

Hinweise für Redakteure:

https://www.enisa.europa.eu/activities/cert/support/awa

https://www.enisa.europa.eu/activities/cert/support/proactive-detection

Für Interviews: Cosmin Ciobanu, NIS Experte, **E-Mail:** Cosmin.Ciobanu@enisa.europa.eu, **Telefon:** (+30) 2814 409663