DE Version

Neuer Sicherheitsstandard für IT-Produkte veröffentlicht

Schulterschluss von cyberintelligence.institute (CII) und EICAR: Gemeinsame Entwicklung des neuen "Product Cybersecurity Standard" (PCS) für mehr produktbezogene Cybersicherheit

Frankfurt, 23. Januar 2025: Das cyberintelligence.institute stellt gemeinsam mit der European Expert Group for IT-Security (EICAR) den neuen "Product Cybersecurity Standard" (PCS) vor. Der neue Sicherheitsstandard für IT-Produkte ist die Weiterentwicklung des „EICAR Minimum Standards“ und will aktiv dabei unterstützen, flächendeckend produktbezogene „Security by Design“ durch die Festlegung grundlegender allgemeingültiger Sicherheitsanforderungen zu realisieren. Ziel des PCS ist nicht nur die generelle Verbesserung der Vertrauenswürdigkeit von IT-Produkten, sondern es soll insbesondere auch der fatalen Sicherheitslage im IoT-Sektor Rechnung getragen werden. CII und EICAR rufen daher gemeinsam Hersteller, Importeure und Vertriebsunternehmen von IT-Produkten auf, sich öffentlich zu den Grundwerten des PCS zu bekennen. Unternehmen können ihr Commitment für mehr produktbezogene Cybersicherheit durch ein entsprechendes Siegel nachweisen

Ohne hinreichend sichere Produkte kann es keine hinreichend sicheren Prozesse geben: In aller Regelmäßigkeit machen sich Cyberangreifer die fehlende IT-Sicherheit von vernetzten Produkten zunutze, um erfolgreich IT-Systeme und Computernetzwerke zu kompromittieren. Das hat zur Folge, dass Unternehmen mit Sicherheitslücken in ihrer IT konfrontiert werden, über die sie oft keine Kenntnis oder Kontrolle haben. Das produktbezogene Sicherheitsrisiko, das eigentlich Aufgabe der Hersteller ist, wird auf diese Weise auf die Anwender und Nutzer abgewälzt, wodurch mangels Kenntnisse und Ressourcen erhebliche Cyberbedrohungen entstehen können. Um diesem Missstand zu begegnen, hat die Europäische Union Regelungen wie den „Cyber Resilience Act“ (CRA) auf den Weg gebracht, um für alle Produkte mit digitalen Elementen zukünftig höhere Sicherheitsstandards zu gewährleisten.

Der neue "Product Cybersecurity Standard" (PCS) unterstützt bei der Umsetzung von „Security by Design“ in IT-Produkten, also der Berücksichtigung von Cybersicherheit ab dem Beginn der Entwicklung bis hin zu deren Abkündigung vom Markt, indem er grundlegende Vorgaben definiert, was datensichere und datenschutzkonforme digitale

und vernetzte Produkte unter Berücksichtigung der aktuellen digitalen Bedrohungslage auszeichnet. Ein solches Set an Anforderungen ist einerseits hilfreich bei der zeitnahen Vorbereitung der Umsetzungsmaßstäbe des CRA, andererseits unterstützt es Unternehmen dabei, durch eine zunächst freiwillige öffentliche Selbstverpflichtung aktiv damit zu beginnen, die Grundlagen für eine höhere IT-Sicherheit ihrer Produkte

zu schaffen und damit der gestiegenen Herstellerverantwortung im Bereich der IT-Sicherheit gerecht zu werden. Hierdurch trägt der PCS zu mehr flächendeckender produktbezogener Cybersicherheit bei.

Was stellt der Standard dar und welche Phasen wird er durchlaufen?

Der Standard definiert produktübergreifende Anforderungen an Security by Design von vernetzten IT-Produkten.

Dabei berücksichtigt er u.a. nachfolgende Aspekte:

- Absicherung der digitalen Lieferkette
- Kontrolle über den Source Code und die Datenverarbeitung
- Einhaltung von Datensicherheits- und Datenschutzanforderungen
- Patch Management sowie Bereitstellung von CVD Policies
- Notfallmanagement
- Legal Compliance
- Schutz vor Backdoors und nicht veröffentlichten Produktfunktionen
- Auslandsdatenübertragung
- Transparenz, Produktdokumentation und Anwenderinformation

Prof. Dr. Dennis-Kenji Kipker: „Die EICAR war mit der Entwicklung ihres Minimum Standards ihrer Zeit voraus. Wir haben die Arbeit, die bereits in den Standard eingeflossen ist, um entsprechende Aktualität ergänzt. Entstanden ist ein zeitgemäßes Konzept von „Security by Design“, das dazu beitragen soll, die produktbezogene Cybersicherheit flächendeckend zu verbessern.“

„Die Zusammenarbeit mit dem cybrintelligence.institute war fachlich und inhaltlich ausgezeichnet“, kommentiert Rainer Fahs, Chairman der EICAR. „Die Einbettung des Minimum Standards in das Konzept der Security by Design ist sinnvoll und der logische nächste Schritt seiner Weiterentwicklung. Die Zeit war reif für diesen Schulterschluss.“

Der Product Cybersecurity Standard kann ab dem 23. Januar sowohl unter www.cyberintelligence.institute/PCS als auch auf der EICAR-Webseite (www.eicar.org) eingesehen werden.

Kurzprofil CII: Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanke sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein. Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.

Kurzprofil EICAR: Die EICAR wurde 1991 als eingetragener Verein in Deutschland gegründet. Zunächst mit dem Ziel, Know-how im Bereich der Antivirenforschung zu bündeln, gilt die EICAR mittlerweile als anerkanntes IT-Security Expertennetzwerk. Das Institut versteht sich als Plattform für den Informationsaustausch für alle Sicherheitsexperten, die in den Bereichen Forschung und Entwicklung, Implementierung sowie Management tätig sind. Hierdurch soll die globale Zusammenarbeit im Bereich der Computersicherheit gefördert werden. Ziel des Instituts ist es, Lösungen und Präventivmaßnahmen gegenüber allen Arten der Computerkriminalität, wie z.B. das Schreiben und Verbreiten von Computer-Viren, Betrug sowie das Ausspähen von personenbezogenen Daten, zu entwickeln. Dabei arbeitet das Institut sowohl sehr eng mit Unternehmen, politischen Organisationen oder universitären Einrichtungen als auch Medien, Technik- und Rechtsexperten zusammen.

Pressekontakt CII:
Prof. Dr. Dennis-Kenji Kipker
Research Director
E-Mail: info@cyberintelligence.institute
Telefon: 069 505034 602

Pressekontakt EICAR:

Manuel Hüttl
EICAR Director Communication
E-Mail: dirbus@eicar.org
Telefon: 0160-5545152