

Cyber Resilience Act

Changes and Challenges for Manufacturers

The information contained in this article has been carefully compiled but cannot replace legal advice. No liability or guarantee is assumed that the work results or information fulfil the requirements of the current legal situation. The same applies to the suitability, completeness or accuracy, so that any liability for damages that may arise from the use of these work results or information is excluded. This limitation of liability shall not apply in cases of wilful intent.

Crosscutting Regulation for Cybersecurity Regulating Products with Digital Elements

Applies to all Products with Digital Elements

- Software
 - Software in a box
 - Apps
 - Software installed in products, e.g. firmware
- Hardware

ATHENE

- Home and SoHo routers
- Industrial production machines
- Remote processing solutions
 - Remote parts of products with digital elements

No exceptions for SME, tiny apps, etc!





Crosscutting Regulation for Cybersecurity Regulating Products with Digital Elements

Exceptions

- Products under <u>listed</u> sector-specific regulations
 - Medical products
 - Civil aviation products
 - Car certification & road safety
 - National security and military products
 - ...

ATHENE

- SaaS services not applicable
 - Pure cloud solutions without a product run by customer





Composite and Imported Products Who is Responsible?







Composite and Imported Products Who is Responsible?







Composite and Imported Products Who is Responsible?







Core Pillars of the CRA Security and Resilience Along the Product Lifecycle

		Annex I		Designed
	ESSENTIAL CYBERSECURITY REQUIREMENTS			Designed
Part I	Cybe			
	elements			Developed
	(1) Products with digital elements shall be designed, developed and produced in			
		such a way that they ensure an appropriate level of cybersecurity based on the risks;		Produced

- SIT-Restricted -



ATHENE

Core Pillars of the CRA Security and Resilience Along the Product Lifecycle

Designed Design Develo Develo Develo Develo Implen Secure Provisi Allow f Handle

ATHENE

- Develop a risk model
- Design for essential cybersecurity requirements
- Develop without known vulnerabilities
- Implement with essential cybersecurity requirements in mind
- Secure default configurations
- Provision current version
- Allow for secure updates
- Handle incidents and vulnerability reports







Spotlight: Risk Model The Foundation for Designing and Implementing Measures



Smart TV

VS.

User Authentication

- Physical access / short range remote control
- Internet services

Consequences of Unavailability

Miss a football match

ATHENE



Industrial Production

User Authentication

- Remote control
- Unauthorized staff in same machine shop?

Consequences of Unavailability

Loss of production

- SIT-Restricted





Seite 10

Spotlight: Risk Model The Foundation for Designing and Implementing Measures



- No authentication for local users
- No access over the Internet

Present badge (NFC) on site

- SIT-Restricted

Username/password for remote access



ATHENE

Validate Against Intended Use Make Clear What The Product is For









Spotlight: Without Known Vulnerabilities Have Your Dependencies in Check

- (2) On the basis of the *cybersecurity* risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
 - (a) be made available on the market without known exploitable vulnerabilities;



What is a known vulnerability?

- SIT-Restricted -

ATHENE



Check Dependencies Against CVEs Need to Know Your Dependencies

Large Dependency Trees

- Dependencies have other dependencies
- Even mid-size projects escalate quickly

Link to CRA

- Only first-level dependencies required in SBOM
- Each node may have vulnerabilities

Security Context

Vulnerabilities

ATHENE

- Known CVEs
- End-of-life components
- Supply chain attacks: where to obtain software from?





SBOM as Part of Vulnerability Handling Not Only a Catalog

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

 identify and document vulnerabilities and components contained in products *with digital elements*, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;







Automatically Generate SBOM Integrate into Development Process

	"\$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json"
<pre>(dependencies)</pre>	"bomFormat": "CycloneDX",
<pre></pre>	om/artifact/commons_io/commons_io
(dependency)	"serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b
(apounTd)commons_io(/apou	"version": 1,
(antifactId)commons_io(/a	"components": [
	[INFO] maven-dependency-plugin:2.8:tree (d/ {
(/dependency)	[INFO] org.soot-oss:soot:jar:4.6.0-SNAPSHOT "type": "library",
(dependency)	<pre>[INFO] +- commons-io:commons-io:jar:2.7:compil("name": "acme-library",</pre>
<pre></pre>	[INFO] +- org.smali:dexlib2:jar:2.5.2:compile "version": "1.0.0"
<pre></pre>	<pre>[INFO] +- com.google.code.findbugs:jsr305:j; }</pre>
(vension)2 5 2//vension)	[INFO] \- com.google.guava:guava:jar:27.1-a]
(dopondoncy)	[INFO] +- com.google.guava:failureaccess }
(dependency)	[INFO] +- com.google.guava:listenablefuture:jar:9999.0-empty-to-avoid-conflict-with-guava:compile
(gnounId)ong_ou2_osm(/gno	[INFO] +- org.checkerframework:checker-compat-qual:jar:2.5.2:compile
<pre></pre>	<pre></pre>
(vonsion) \$ [asm vonsion] //	<pre>// [INFO] +- org.ow2.asm:asm:jar:9.7:compile</pre>
(dependency)	[INFO] +- org.ow2.asm:asm-tree:jar:9.7:compile
<pre></pre>	[INFO] +- org.ow2.asm:asm-util:jar:9.7:compile
<pre><dependency></dependency></pre>	[INFO] \- org.ow2.asm:asm-analysis:jar:9.7:compile
<pre><groupid>org.ow2.asm</groupid></pre>	[INFO] +- org.ow2.asm:asm-commons:jar:9.7:compile
<artifactid>asm-tree<td><pre>/ [INFO] +- org.javassist:javassist:jar:3.28.0-GA:provided</pre></td></artifactid>	<pre>/ [INFO] +- org.javassist:javassist:jar:3.28.0-GA:provided</pre>
<pre><version>\${asm.version}</version></pre>	[INFO] +- xmlpull:xmlpull:jar:1.1.3.4d b4 min:compile
	[INFO] +- org.apache.ant:ant:iar:1.10.11:provided
	[INFO] \- org.apache.ant:ant-launcher:jar:1.10.11:provided
	[INFO] +- de.upb.cs.swt:axml:iar:2.1.3:compile
	r





Essential Cybersecurity Requirements Concrete Measures Depend on Risk Analysis

Annex I

ESSENTIAL CYBERSECURITY REQUIREMENTS

- On the basis of the *cybersecurity* risk assessment referred to in Article 13(2) (2)and where applicable, products with digital elements shall:
 - be made available on the market with a secure by default configuration, (b) unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;



SIT

ATHENE



Essential Cybersecurity Requirements Areas of Required Measures

Secure Standard Configuration

Ability to restore settings to default

Authentication

Controls against unauthorized access

Confidentiality

- All data, not only personal data (as in GDPR)
- Protection of data in storage, transit or being processed

Integrity

- All data, not only personal data (as in GDPR)
- Includes programs, commands, configuration

Data Reduction

- All data, not only personal data (as in GDPR)
- Reduce the data being processed to what is necessary

Availability

Preserve availability of essential features even under DoS attack

Reduce Negative Impact

- Reduce effect on other devices on the network
- Reduce exploitability

Reduce Attack Surface

Provide Logging

Seite 18

Allow Security Updates





Checking The Own Code Avoiding Vulnerabilities During Development







Spotlight: Code Scanning Possible During Development Process

Dashboard			API Docs 🏼 🌣 Settings
Search			
	soot-4.5.0-jar-with	Servlet.class	InsecureBankv2.apk Version: 1.0
	soot-4.5.0-jar-with-depen	Servlet.class	InsecureBankv2
Drop files here	Additional analyses	i Additional analyses	i Additional analyses
or click to upload	28 4 1	0 0 0	45 58 30
WebGoat-6.0.1.war Version: 2.5	com.meamobile.printi Version: 3.1.4		
WebGoat	Printicular		
i Additional analyses	Additional analyses		
353 3 17	639 180 141		





Spotlight: Code Scanning Vulnerability Categories on Example

	Drintia	ular								Vuln	erabilit	ies
	com.meamo	uldi obile.printicular-72.apk Version:	3.1.4				Submissic Finished :	on : 24 Apr 2024 22:28:5 25 Apr 2024 06:22:45	ⁱ¹ 6	539	180	141
	Vulnerabilities	Communications	App Info	Dynamic Runs				Show Findings in	n: 🔽 Lib	oraries	🖸 Apj	p Code
					Search: Search vulnerabilitie	Name	>	Filter by	severity:	Select	severiti	ies 👻
1	Backend Credentia	ls in Code										\sim
	Cryptography											\sim
	Hardening											\sim
	Inter-Component C	Communication										\sim
	Libraries											\sim
	Network											\sim
	Permissions											\sim
	Storage											~





Spotlight: Code Scanning Vulnerability Details on Example

	de		
Hard-Coded Backend	Credentials for AWS	:	
Description			
he app connects to a Am	azon Web Service (AWS)	database backend using hard-coded credentials.	
/litigation			
lever place backend cred	entials into the app. Use a	trusted middleware to connect to the database instead. Ensure that this middleware applies proper authenticat	ion and authorization.
References:			
<u>The app does not rely on</u>	symmetric cryptography	with hardcoded keys as a sole method of encryption. Mobile Application Security Verification Standard as define	d by OWASP (Open We
Application Security Proje	Ct) 3.1		
Application Security Proje Guide on how to test the	ct) 3.1 <u>key management</u>		
Application Security Proje Guide on how to test the Location:	key management	✓ Verify ▼	
Application Security Proje Guide on how to test the Location: Vulnerability was found	key management	✓ Verify ▼	Jump to Code
Application Security Proje Guide on how to test the Location: Vulnerability was found in class com.meamobil	key management key management e.photoserviceandroida	✓ Verify ▼ pi.photocreate.api.ImagesAPI\$S3Connector	Jump to Code
Application Security Proje Guide on how to test the Location: Vulnerability was found in class com.meamobil in method java.lang.Stu	e.photoserviceandroida ing dolnBackground(jav	✓ Verify ▼ pi.photocreate.api.ImagesAPI\$S3Connector va.lang.String[])	Jump to Code
Application Security Proje Guide on how to test the Location: Vulnerability was found in class com.meamobil in method java.lang.Stu in statement specialinv	e.photoserviceandroidaj ing doInBackground(jav oke \$BasicAWSCredentia	✓ Verify ▼ pi.photocreate.api.ImagesAPI\$S3Connector va.lang.String[]) als5. <com.amazonaws.auth.basicawscredentials: <init="" void="">(java.lang.String.java.lang.String)>(\$String&</com.amazonaws.auth.basicawscredentials:>	
Application Security Proje Guide on how to test the Location: Vulnerability was found in class com.meamobil in method java.lang.Str in statement specialinv Additional data:	key management e.photoserviceandroida ing doInBackground(jav oke \$BasicAWSCredentia	va.lang.String[]) als5. <com.amazonaws.auth.basicawscredentials: <init="" void="">(java.lang.String,java.lang.String)>(\$String</com.amazonaws.auth.basicawscredentials:>	Jump to Code
Application Security Proje Guide on how to test the Location: Vulnerability was found in class com.meamobil in method java.lang.Str in statement specialinv Additional data: Access Key:	e.photoserviceandroida ing doInBackground(jav oke \$BasicAWSCredentia	<pre>verify ~ pi.photocreate.api.ImagesAPI\$S3Connector va.lang.String[]) als5.<com.amazonaws.auth.basicawscredentials: <init="" void="">(java.lang.String,java.lang.String)>(\$String{200VG33W4GNA</com.amazonaws.auth.basicawscredentials:></pre>	Jump to Code





Models and Code

Integrating Vulnerability Scanning and Risk Model

Analyze Effect of Vulnerabilities

- Link code scanner results to risk model
- Identify affected assets
- Assess attack complexity

Attack Trees

- Model potential attack paths
- Each node is an intermediate goal
- Vulnerabilities help realize intermediate goals

Automatic Matching

ATHENE

- Based on MITRE ATT&CK
- Prototype shown at Fraunhofer booth





GDPR and CRA – Check Your Data Use Example on the Map







Coordinated Vulnerability Disclosure Mandated by the CRA





Reporting Responsibilities Deadlines for Official Reporting

Within 24 Hours: Early Warning

Affected member states where the product was made available

Within 72 Hours: Vulnerability Notification (if Exploited)

- Affected product
- General nature of the exploit
- Vulnerability concerned
- Corrective or mitigating measures taken
- Measured available to users

Within 14 Days: Final Report

- Description of vulnerability & its severity and impact
- If available: Information on malicious actor
- Details about security update or corrective measures











Orthogonal to Other Regulation Other Duties May Apply

GDPR

- May require reporting to data protection authority
- May require informing the data subject

NIS-2 Directive and National Law

Applies to critical infrastructure

DORA

ATHENE

Banking and financial sector

datenschutz. hessen.de	r hessen.de 🕅 🗃
	Startseite – Service – Meldung nach Art. 33 DS-GVO
≡ Menü	Art. 33 DS-GVO
Q Suche	Meidungen von verletzungen des Schutzes personenbezogener Daten durch
Medienraum	Verantwortliche
Themen A-Z Beschwerde	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit stellt für Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 DS-GVO ein entsprechendes Formular zum Download bereit.
Datenpanne Datenschutzbeauftragte	➡ Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 DS- GVO (DOCX/89.26 KB)
	Sie haben die Möglichkeit das Formular lokal, das heißt ohne geöffnetes Browser-Fenster, auszufüllen. Anschließend können Sie einen Upload-Link anfordern, über den Sie das ausgefüllte Formular an den Hessischen Beauftragten für Datenschutz und Informationsfreiheit übermitteln können. Hierzu wird <i>HessenDrive</i> als sichere Plattform zum Dokumentenaustausch eingesetzt. Nachfolgend finden Sie Informationen zur Nutzung der Plattform.

- SIT-Restricted -



×

Dates and Fines What if we don't get it right?

Essential Cybersecurity Requirements

- Fine up to 15,000,000 EUR
- Up to 2,5% of total worldwide annual turnover

Documentation and Formals

- Fine up to 10,000,000 EUR
- Up to 2% of total worldwide annual turnover

Failure in Reporting Duties

Fine up to 5,000,000 EUR

ATHENE

Up to 1% of total worldwide annual turnover







Contact

Dr.-Ing. Steven Arzt Head of Department Secure Software Engineering Tel. +49 6151 869-336 Fax +49 6151 869-224 <u>steven.arzt@sit.fraunhofer.de</u>

Fraunhofer SIT Rheinstraße 75 64295 Darmstadt www.sit.fraunhofer.de

Fraunhofer SIT Visit us! Hall 6, booth 314