Lerneinheit

[Schutz von Hardware und Software]

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Schutz von Hardware und Software

Einführung

Hardware und Software sind miteinander verbunden: Ohne Software hätte die Hardware eines Computers keine Funktion.

Die Digitalisierung verändert unsere Volkswirtschaften weltweit. Ob bei der Arbeit oder im Privatleben, es gibt immer wieder Fragen zur Hard- und Software, die uns alle betreffen. Darüber hinaus müssen Hard- und Software regelmäßig aktualisiert, aufgerüstet oder ersetzt werden, da ernsthafte Risiken für Organisationen und auch für die Gesellschaft insgesamt bestehen.

In dieser Content-Einheit erfahren Sie etwas über die häufigsten Angriffe, die Hard- und Software betreffen, und was Sie tun können, um sich davor zu schützen.

Wissen Sie, dass die meisten Probleme Softwareprobleme sind? Zum Beispiel kann Computersoftware aus verschiedenen Gründen versagen, weil Viren- und/oder Malware-Infektionen auf Ihrem Computer sehr häufig vorkommen, weil Menschen oft etwas herunterladen oder einklicken, das darauf abzielt, Ihrem Computer Schaden zuzufügen. Es gibt viele Möglichkeiten, Software-Probleme zu beheben, wie Deinstallieren und Neuinstallieren, Aktualisieren, Verwenden von aktualisierter Antiviren-Software und Überprüfen der Website des Herstellers auf Patches. Aber es gibt noch mehr, was Sie tun können, wie Sie in dieser Inhaltseinheit sehen werden.

Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Nachdem Sie sich durch diese Inhaltseinheit gearbeitet haben, kennen Sie die häufigsten Arten von Angriffen auf Hard- und Software und wissen auch, was Sie tun können in Form von Tipps und Empfehlungen, die Sie regelmäßig anwenden können, um einen besseren und sichereren Hard- und Softwareschutz zu erhalten.

Co-funded by the
Erasmus+ Programme
of the European Union

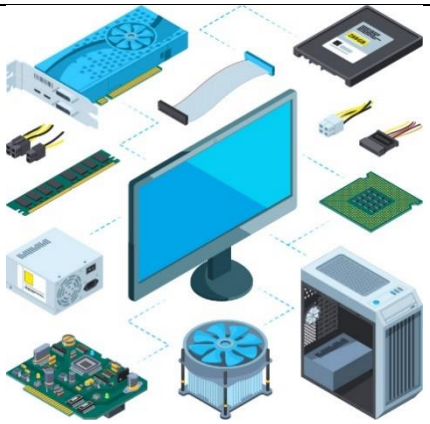
1.Wissen aufbauen - Hardware und Software und die häufigsten Angriffe

Die Digitalisierung verändert unsere Volkswirtschaften weltweit. Trotz der zahlreichen Vorteile, die sich aus diesem Phänomen ergeben, gibt es auch **zunehmende Bedrohungen für die digitale Sicherheit**, die die Sicherheit und Privatsphäre in unseren Wohnungen, Autos, Unternehmen oder sogar Netzwerken beeinträchtigen. Das liegt daran, dass wir im Alltag ständig digitale Geräte verwenden, ein Trend, der ständig zunimmt.
Daher muss die Hard- und Software dieser Geräte häufig **aktualisiert, aufgerüstet oder ersetzt** werden, da ernsthafte Risiken und Bedrohungen für die gesamte Gesellschaft bestehen.

Aber lassen Sie uns bei Null anfangen: Worauf genau beziehen wir uns, wenn wir über Hard- und Software sprechen? In der untenstehenden Tabelle finden Sie eine detaillierte Definition von Hard- und Software.

Definition
Hardware ist jede **physische Komponente**, die in oder mit Ihrem Gerät verwendet wird, während Software das ist, was Sie in der Festplatte, dem Smartphone und/oder Tablet Ihres Computers haben. Hardware ist der Teil Ihres **Computers oder Smartphones**, wohingegen Software Daten auf der Festplatte Ihres Computers sammelt und verarbeitet. Einige Beispiele für Hardwarekomponenten sind: Computerprozessor (CPU), Festplatte, Hauptplatine, Computermonitor, Drucker oder eine Maus. **Software** ist der **logische Teil** Ihres Computers oder Smartphones; sie kann nicht berührt werden, da sie immateriell ist. Dennoch verwendet j**ede Software mindestens eine Hardware-Komponente zum Betrieb**. Sie können sich Software als eine Reihe von Anweisungen vorstellen, die einem Gerät genau sagen, was es tun soll. Das können Programme oder Daten sein. Zum Beispiel ein Videospiel und Microsoft Outlook.

Um es für Sie deutlicher zu machen, sehen Sie in der folgenden Tabelle nun die Hauptunterschiede zwischen Hardware und Software:

	Hardware	Software
		
Funktion	Hardware ist ein **physischer Teil** eines physischen Geräts, der für die	Software ist **eine Reihe von Anweisungen**, die einem Computer genau sagen, was er tun soll.

	Verarbeitung von Daten/Informationen verantwortlich ist Hardware **kann ohne Software nicht funktionieren**	Software ist dafür **verantwortlich, dass die Hardware funktioniert**
Merkmale	Hardware sind physische elektronische Geräte, die wir sehen und berühren können Hardware kann nicht von Computerviren befallen werden	Wir können die Software sehen und auch benutzen, aber wir können sie nicht anfassen Software ist **von Computerviren betroffen**
Lebenszyklus	Sie können körperlich beschädigt werden	Sie können veralten
Initialisierung	Sie funktionieren, sobald die Software installiert ist.	Sie müssen in der Hardware installiert sein, damit sie funktionieren
Wartung	Stücke können von einem Ort an einen anderen übertragen werden	Sie können neu installiert und übertragen werden.
Beispiele	Maus, CPU, Monitor, Drucker, Festplatte usw.	Microsoft Word, Firefox, Skype, Adobe Reader usw.

Wie wir in der vorstehenden Tabelle sehen können, sind **Hardware und Software miteinander verbunden**, und ohne Software hätte die Hardware eines Computers keine Funktion.

Hard- und Softwareschutz ist gerade in der heutigen Zeit für alle ein heißes Thema geworden. Aber warum ist das so? In der folgenden Tabelle sehen Sie drei Hauptzwecke des Hard- und Softwareschutzes.

Hardware-Schutz	Software-Schutz
1. Computer-Hardware kann sehr zerbrechlich sein (z.B. Hitze, Wasser, unsachgemäßer Gebrauch, von Menschen verursachte physische Unfälle sind die größten Bedrohungen für die physische Sicherheit eines Computers)	1. Regelmäßige Software-Updates haben viele Vorteile wie die Vermeidung von Computerfehlern, Schwächen in Softwareprogrammen oder Betriebssystemen
2. Die Hardware sollte ordnungsgemäß sauber sein, um sie vor übermäßiger Hitze zu schützen.	2. Software-Updates helfen beim Umgang mit Sicherheitsmängeln/Schwachstellen
3. Einige Vorfälle wie z.B. ein Raubüberfall, Wasser in Ihrer Hardware kann zu Verlust/Diebstahl von Daten und Informationen führen und Ihr System und Ihre Datendateien beschädigen.	3. Software hilft, Ihre Daten/ wertvollen Informationen vor externen Malware-Quellen zu schützen

Daher spielen Hardware- und Softwaresicherheit eine wichtige Rolle bei der Gewährleistung von Vertrauen, Integrität und Authentizität. **Kommen wir nun zu einigen Beispielen, die deutlich machen, warum der Schutz von Hard- und Software entscheidend ist!**

Beispiel

Co-funded by the
Erasmus+ Programme
of the European Union

Wussten Sie, dass Sony Pictures 2011 von einer Hackergruppe angegriffen wurde, die rund 1 Million Benutzerkonten mit persönlichen Daten (Passwörter, E-Mails, Privatadressen, Geburtsdaten usw.) freigab und damit die Datenschutzrichtlinien ihres Dienstes verletzte?

Im Jahr 2017 wurde der HBO-Riese angegriffen, und der Hacker veröffentlichte das Drehbuch einer Episode einer sehr populären Fernsehserie (Game of Thrones), die nicht ausgestrahlt worden war, und verschaffte sich zudem Zugang zu Finanzdokumenten, zur Kontaktliste der Besetzung und der Crew sowie zu anderen vertraulichen Informationen.

Diese Art von Vorfällen kann vermieden werden, wenn man einen starken Software- und Hardwareschutz hat.

1. Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist die Bedeutung von Hardware und Software?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Software ist ein Teil des Computers, der berührt werden kann.
- Hardware kann von Computerviren befallen werden.
- Die Software ist dafür verantwortlich, dass die Hardware funktioniert.
- Hardware und Software funktionieren nur, wenn sie zusammen sind.

Übung MULTIPLE CHOICE

Situation: Bezüglich Hardware- und Softwareschutz wählen Sie bitte die richtigen Sätze aus.
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die häufigsten Angriffe auf Hardware werden hauptsächlich durch externe Quellen verursacht.
- Der Softwareschutz muss regelmäßig durchgeführt werden.
- Software-Angriffe sind die häufigsten, deshalb sollten Sie nach mehrfachen Software-Schutzmaßnahmen suchen.
- Software muss durch einen Virenschutz geschützt werden.

2.Wissen aufbauen - Besserer Schutz der Hardware

Nachdem Sie nun wissen, was Hard- und Software ist und warum Sie sie schützen sollten, lernen Sie in den nächsten beiden Kapiteln typische Angriffe auf Hard- und Software und Maßnahmen zur Vermeidung beider kennen.

Auf den folgenden Seiten werden Sie mit den häufigsten Angriffen auf Hardware in Berührung kommen, und um Ihnen zu helfen, sich zu schützen, geben wir Ihnen einige Tipps und Empfehlungen, um sich vor Hardware-Problemen zu schützen.

Zunächst müssen Sie aber wissen, was Hardware-Schutz ist und was die häufigsten Angriffe auf Hardware sind.

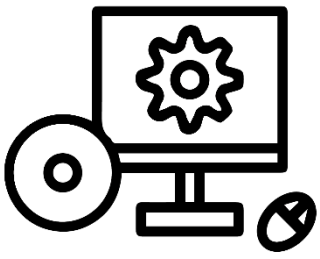
Der Hardwareschutz bezieht sich auf den **Schutz der physischen Geräte**, der von einer Person durchgeführt werden muss.

Aber was sind die häufigsten Angriffe auf Hardware?

Es gibt drei Angriffe, die häufiger vorkommen. Die beiden am häufigsten auftretenden Probleme sind in der folgenden Tabelle aufgeführt:

HARDWARE	
Physische Unfälle	**Änderung**
Physische Unfälle, wie z.B. Wassertropfen in einer physischen Komponente oder unsachgemäßer Gebrauch, können von Menschen verursacht werden. Diese Art von Hardware-Problemen kann die physische Sicherheit von Computern gefährden.	Modifizierung von Hardware, Software oder irgendetwas anderem, um eine Funktion auszuführen, die nicht ursprünglich vom ursprünglichen Designer/künftigen Besitzer der Hardware konzipiert oder beabsichtigt war

Zum Beispiel sind die **Hauptfolgen gängiger Angriffe auf Hardware**:

Modding 	**Böswillige Hardware-Modifikationen** von InsiderInnen stellen eine ernsthafte Bedrohung dar. Daher ist es wichtig, die Originalquelle zu kennen, wo Sie Hardware-Komponenten kaufen. Beispielsweise können sich kritische Infrastrukturkomponenten wie Mikroprozessoren in Ihrem Computer befinden, um Sie zu kontrollieren.
Physische Unfälle 	Hardware kann sehr zerbrechlich und auch sehr wertvoll sein. Hitze, Feuchtigkeit, Vibrationen, extreme Temperaturen, Staub, Wasser und physische Unfälle mit physischen Komponenten sind eigentlich die größten Bedrohungen für die physische Sicherheit eines Computers. Daher müssen Sie Ihre gesamte Hardware ordnungsgemäß gereinigt halten, weit entfernt von übermäßigen Wärmequellen, und Sie sollten Flüssigkeiten fern von Computern, Smartphones und Tablets aufbewahren.

Nachdem Sie wissen, was mit Ihrer Hardware passieren kann, müssen Sie neugierig darauf sein, welche Tipps und Empfehlungen Sie verwenden können, um Ihre Hardware sicher zu verwahren.

In der **folgenden Liste** finden Sie einige Schritte zum Schutz Ihrer Hardware:

1. **Hardware-Modifikationen sind illegal**, es sei denn, Sie sind mit dieser Art von Änderungen einverstanden. Zum Beispiel können Sie, wenn Sie wollen, einige Änderungen an Ihrem Computer vornehmen, um etwas zu verbessern (Geschwindigkeit, Kapazität usw.). Aus diesem Grund müssen Sie es **vermeiden, Hardware-Komponenten aus risikoreichen Quellen/Ländern** wie Online-Plattformen **zu kaufen**, die der Allgemeinheit noch unbekannt sind, auch wenn der Preis sehr niedrig und attraktiv ist, denn normalerweise kann Hardware, die aus nicht vertrauenswürdigen Quellen stammt, ein Sicherheitsrisiko darstellen;
2. Es gibt auch **spezielle Nachverfolgungssysteme**, mit denen Sie z.B. feststellen können, ob Ihre Hardware gestohlen wurde oder verloren gegangen ist;
3. Um gut auf Ihre Hardware aufzupassen, sollten Sie immer **aktuelle Sicherheitssoftware installieren und verwenden**. Dieser Tipp wird ausführlicher sein, nachdem wir über den Softwareschutz gesprochen haben;
4. **Vermeiden Sie es, Ihre Hardware auf hohen Flächen und weit entfernt von Wärmequellen, Wasser und Stromkreisen aufzustellen;**
5. **Reinigen Sie Ihre Hardware sehr vorsichtig** mit einem trockenen Tuch oder einem speziellen Werkzeug, wie einer Bürste mit langem Stiel und weichen Borsten, Wischtüchern, die Sie in speziellen Geschäften kaufen können, die Hardware-Zubehör verkaufen. Behalten Sie diesen Tipp als Ihre Wartungsregel und so oft wie nötig.

2. Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist die Bedeutung des Hardwareschutzes?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Der Hardwareschutz hängt nur von Personen ab.
- Hardware-Schutz ist das, was eine Person tun kann, um die physischen Komponenten zu schützen.
- Hardwareschutz kann nicht nur von einer Person durchgeführt werden.
- Hardwareschutz bezieht sich nur auf die Durchführung von physischen Aktionen/Maßnahmen.

Übung MULTIPLE CHOICE

Situation: Was kann im Falle eines Hardware-Angriffs geschehen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Der häufigste Angriff auf Hardware bezieht sich nur auf nicht autorisierte physische Veränderungen.
- Physische Unfälle passieren häufiger, weil Menschen manchmal unverantwortliche Verhaltensweisen/Handlungen an den Tag legen.
- Angriffe auf Hardware können die persönlichen Daten und die physische Sicherheit des Hardwarebesitzers gefährden.
- Hardware-Angriffe stehen im Zusammenhang mit physischen Vorfällen und der Veränderung von Hardware.

Übung MULTIPLE CHOICE

Situation: Welche Empfehlungen können bezüglich des Hardwareschutzes umgesetzt werden?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Halten Sie Ihre Hardware sauber und fern von Hitze- und Wasserquellen.
- Der Hardwareschutz sollte durch einen Softwareschutz ergänzt werden.
- Sie sollten den Kauf von Hardwarekomponenten aus risikoreichen Quellen/Ländern wegen möglicher unerwünschter Änderungen vermeiden.
- Personen können bei Bedarf spezielle Verfolgungssysteme und selbstzerstörende Geräte verwenden.

3.Wissen aufbauen - Besserer Softwareschutz

Es ist jetzt an der Zeit, mehr über Softwareschutz zu erfahren, besonders weil es viele Angriffe gibt, die passieren können. Heutzutage werden verschiedene Softwaretypen von uns allen benutzt, und manchmal merken wir das gar nicht.

Jetzt, da Sie wissen, was Hardwareschutz ist, sollten Sie auch die Definition von Softwareschutz kennen.

Softwareschutz ist eine **Architektur und Methodik für die Sicherheit von Computernetzwerken**, die Sicherheitsvorrichtungen und defensiven Schutz aus (externen und internen) Quellen kombiniert. Softwareschutz erfordert eine Kombination von Techniken, die sich auf unterschiedliche Software beziehen. Softwareschutz ist heute ein kritischer Aspekt nicht nur für Unternehmen, sondern auch für Einzelpersonen.

Doch was sind die häufigsten Angriffe auf Software?

Auch wenn es eine Vielzahl von Angriffen auf Software gibt, finden Sie in der Tabelle unten die häufigsten Angriffe.

SOFTWARE			
Trojan	**Malware**	**Virus**	**Phishing**
Computerprogramm, das sich Zugang zu einem Computer oder System verschafft, das in Form von normaler Software getarnt ist, um Systemprozesse, Festplattendaten usw. zu beschädigen. Meist über E-Mail-Anhänge eingeführt	Kann Spyware, Ransomware, Viren und Würmer enthalten. Malware entsteht in der Regel durch gefährliche Klicks oder E-Mail-Anhänge, die dann risikoreiche Software installieren.	Computerprogramm, das darauf ausgelegt ist, andere Computerprogramme zu infizieren, wichtige Systemdaten zu zerstören und Netzwerke funktionsunfähig zu machen	Praxis des Versendens betrügerischer Mitteilungen, die scheinbar aus einer vertrauenswürdigen Quelle stammen, in der Regel per E-Mail. Das Ziel ist es, Informationen/Daten von jemandem zu stehlen (z.B. Kreditkarten-, Login-Informationen usw.).
Ransomware	**Würmer**	**Spyware**	**Cryptojacking**
Blockieren Sie den Zugang zu	Malware-Computerprogramm, das sich selbst	Software, die es einem Benutzer ermöglicht, Informationen über	Unbefugte Benutzung eines fremden Computers zum Abbau

Schlüsselkomponenten Ihres Netzwerks	repliziert, um sich auf andere Computer zu verbreiten	die Computeraktivitäten eines anderen zu erhalten	von Krypto-Währung. Diese Angriffe erfolgen über böswillige Links in einer E-Mail, infizieren eine Website oder Online-Werbung.

Zum Beispiel sind die drei **wichtigsten Folgen von häufigen Angriffen auf Software:**

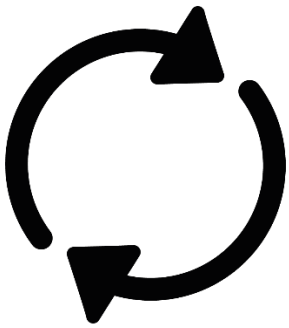
Fehler	Eine häufige Quelle von Software-Sicherheitsmängeln. Einige Fehler stellen Sicherheitslücken dar, die zu einem Informationsleck oder unberechtigtem Zugriff führen können.
Gebrochene Authentifizierung und Versagen beim Datenschutz	Manchmal sind Funktionen im Zusammenhang mit der Authentifizierung fehlerhaft, und deshalb können einige Sicherheitsprobleme auftreten. Diese Situation kann dazu führen, dass nicht autorisierte Personen auf die Konten von BenutzerInnen zugreifen, um deren Identität anzunehmen. In diesem Fall können Personen wichtige Unternehmensinformationen verlieren, und gestohlene persönliche Informationen können dazu verwendet werden, Ihnen und/oder Ihren KundInnen zu schaden.
Unterbrechung von Geschäftsaktivitäten	Ein Angriff auf Software kann Ihr Unternehmen in den Bankrott treiben. Darüber hinaus kann das Vertrauen der KundInnen beeinträchtigt werden, wenn sie wissen, dass sie Opfer eines Angriffs geworden sind.

Nachdem Sie die heutzutage am häufigsten vorkommenden Angriffe auf Software gesehen haben, müssen Sie wissen, was Sie tun können, um diese Art von Vorfällen zu verhindern. Und nachdem Sie einige der häufigsten Angriffe gesehen haben, werden Sie sicher zustimmen, dass der Schutz von Software ein zentrales Thema ist.

Hier finden Sie **einige Hinweise** darauf, was Sie tun können, um sich vor den häufigsten Angriffen auf Software zu schützen:

	Schützen Sie Ihre persönlichen Daten durch die Verwendung **mehrerer sicherer Passwörter und häufiger Backups**. Sie können Informationen auch verschlüsseln. Erstellen Sie mehrere Backups aller Ihrer wichtigen Daten und stellen Sie sicher, dass sie nicht alle am gleichen Ort/an der gleichen Quelle gespeichert sind. Bewahren Sie immer Software-Firewalls auf. Um dies zu tun, sollten Sie Ihre Hardware-Einstellungen überprüfen und Ihre Standard-

	Firewall zusammen mit seriöser Antiviren-Software aktiviert haben.

	**Installieren Sie häufig Updates** und halten Sie Ihre Software immer auf dem neuesten Stand. **Installieren Sie einen Phishing-Filter/eine Phishing-Software** in Ihrer E-Mail-Anwendung und auch in Ihrem Webbrowser. Diese Filter werden zwar nicht alle Phishing-Nachrichten fern halten, aber sie werden die Anzahl der Phishing-Versuche reduzieren. Halten Sie Ihr Betriebssystem und Ihre **Sicherheitssoftware auf dem neuesten Stand.** Führen Sie **regelmäßig geplante Scans** mit Ihrer Antiviren-Software durch und stellen Sie sicher, dass Ihre Antiviren- und Anti-Spyware-Software kompatibel sind.

	**Öffnen Sie niemals einen E-Mail-Anhang** oder führen Sie ein Programm aus, wenn Sie nicht 100% sicher sind, dass es sich um eine sichere Quelle handelt. **Überprüfen Sie die SSL-Zugangsdaten** der Website und verwenden Sie **niemals persönliche/sensible Informationen** auf Websites, die kein gültiges SSL-Zertifikat installiert haben. Um die SSL-Anmeldedaten der Website einzusehen, klicken Sie bitte auf das geschlossene Vorhängeschloss in einem Browserfenster "Klicken Sie auf das Vertrauenszeichen". **Vermeiden Sie die Verwendung öffentlicher Netzwerke.** **Setzen Sie einen Website-Filter** ein, um bösartige Websites zu blockieren. Ein Website-Filter kann Ihnen bei der Kontrolle von Websites helfen, indem er eine Zulässigkeits- oder Sperrliste erstellt. Wie Sie das tun können, erfahren Sie auf dieser Website: www.currentware.com/web-filter.

Wie wir sehen, **ist Vorbeugung der Schlüssel** zur Vermeidung von Software-Problemen, und proaktiv zu sein, mit anderen Worten, einige Maßnahmen zu ergreifen, um sich selbst zu schützen, ist immer die beste Option.
Abschließend ist es wichtig, sich vor Augen zu halten, dass sich die Angriffe jeden Tag weiterentwickeln, und **deshalb müssen Sie über die neuesten Angriffe und Schutzmaßnahmen auf dem Laufenden bleiben**.

Das Hauptziel ist es, auf dem Laufenden zu bleiben, was es an Malware gibt, es geht darum, Ihre Sicherheit zu gewährleisten.

3. Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist die Bedeutung von Softwareschutz?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Kombination von Softwareschutz erfordert eine Kombination aus mehreren Techniken und Methoden.
- Softwareschutz ist meist reaktiv.
- Hardware- und Softwaresicherheit sollte eine Priorität sein, aber Softwareschutz muss häufiger durchgeführt werden.
- Softwareschutz ist wichtiger, weil die Menschen täglich mehr Software benutzen.

Übung MULTIPLE CHOICE

Situation: Was kann im Falle eines Software-Angriffs geschehen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Eine häufige Folge eines Software-Angriffs ist das Informationsleck.
- Eine weitere häufige Folge eines Software-Angriffs ist der unberechtigte Zugriff.
- Es kommt sehr häufig vor, dass bei einem Software-Angriff finanzielle Verluste entstehen.
- Gebrochene Authentisierung und mangelnder Schutz passieren oft gleichzeitig.

Übung MULTIPLE CHOICE

Situation: Welche Empfehlungen können bezüglich Softwareschutz umgesetzt werden?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Man muss mehrere Methoden zum Schutz der Software implementieren und so oft wie möglich Leistungstests durchführen.
- Aktualisierte Firewalls, Antiviren- und Phishing-Filter sind Beispiele für den Schutz der Software.
- Da die Angriffe immer komplexer werden, müssen die Methoden zum Schutz der Anwendung aktualisiert werden.
- Da sich Software-Angriffe weiterentwickeln, sollten auch die Softwareschutzmaßnahmen aktualisiert werden.

Co-funded by the
Erasmus+ Programme
of the European Union

Quellen

Diana, J. (n.d.). *Hardware e Software.* https://www.todamateria.com.br/hardware-e-software/

Hossain, F. R. (July 4 2018). *Importance of Security in Software Development.* Retrieved from https://medium.com/brainstation23/importance-of-security-in-software-development-f92669838a90

Co-funded by the
Erasmus+ Programme
of the European Union

Wissen sichern

Hardware- und Softwareschutz sind wesentliche Aspekte der Sicherheit, **da sie dafür verantwortlich sind, wertvolle Softwarewerte aufgrund von böswilligen Aktivitäten auf Software zu erhalten**.

Obwohl **Hardware und Software miteinander verbunden sind** und ohne Software die Hardware eines Computers nicht funktionieren würde, und umgekehrt, sind Hardware und Software zwei verschiedene Dinge: **Hardware** ist jede **physische Komponente**, die in oder mit Ihrem Gerät verwendet wird, während **Software der logische Teil** Ihres Computers oder eines anderen Geräts ist. Einige Beispiele für Hardware sind die Hauptplatine, ein Computermonitor, ein Drucker oder eine Maus, und einige Beispiele für Software sind ein Videospiel oder ein Programm wie Microsoft Office.

Auch wenn es unmöglich ist, die Möglichkeit eines Hardware- oder Softwarezwischenfalls zu vermeiden, so gibt es doch eine Reihe von Maßnahmen/Tools, die Sie befolgen können, um sich selbst so gut wie möglich zu schützen. Die **Hardware ist menschlichen Fehlern ausgesetzt** und wird ohne die richtige Pflege, wie regelmäßige Aufräumarbeiten und physischer Schutz gegen die Elemente (Wasser, Hitze, Kälte usw.), beschädigt. **Software** ist exponentiell empfindlicher gegenüber externen Bedrohungen: Sie **kann von Cyberattacken** wie Trojanischen Pferden, Viren, Phishing-Angriffen, Spyware, Malware und vielen anderen **betroffen sein**. Daher ist es von entscheidender Bedeutung, dass Sie Maßnahmen ergreifen, um das Risiko von Cyber-Bedrohungen zu minimieren. So müssen Sie beispielsweise mehrere **starke Passwörter und häufige Backups verwenden**, **Software-Firewalls** und einen **aktuellen Virenschutz verwenden** sowie einen **Website-Filter** einsetzen, um bösartige Websites zu blockieren.

Wie wir sehen, ist **Prävention der Schlüssel** zur Vermeidung von Software-Problemen, daher ist die Lösung proaktiv. Mit anderen Worten: Die beste Option ist immer, einige Maßnahmen zu ergreifen, um sich vor Cybersicherheitsbedrohungen zu schützen!

Abschließend ist es wichtig, sich vor Augen zu halten, dass sich die Angriffe ständig weiterentwickeln, und deshalb **müssen Sie über die neuesten Sicherheitsverhaltensweisen und Schutzmaßnahmen auf dem Laufenden bleiben.**

Co-funded by the
Erasmus+ Programme
of the European Union

Lösungsschlüssel
(die korrekten Antworten sind fett markiert)

1.Wissen anwenden

Situation: Was ist die Bedeutung von Hardware und Software?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Software ist ein Teil des Computers, der berührt werden kann.
- Hardware kann von Computerviren befallen werden.
- **Die Software ist dafür verantwortlich, dass die Hardware funktioniert.**
- **Hardware und Software funktionieren nur, wenn sie zusammen sind.**

Situation: Bezüglich Hardware- und Softwareschutz wählen Sie bitte die richtigen Sätze aus.
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die häufigsten Angriffe auf Hardware werden hauptsächlich durch externe Quellen verursacht.
- **Der Softwareschutz muss regelmäßig durchgeführt werden.**
- **Software-Angriffe sind die häufigsten, deshalb sollten Sie nach mehrfachen Software-Schutzmaßnahmen suchen.**
- **Software muss durch einen Virenschutz geschützt werden.**

2.Wissen anwenden

Situation: Was ist die Bedeutung des Hardwareschutzes?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Der Hardwareschutz hängt nur von Personen ab.**
- **Hardware-Schutz ist das, was eine Person tun kann, um die physischen Komponenten zu schützen.**
- Hardwareschutz kann nicht nur von einer Person durchgeführt werden.
- Hardwareschutz bezieht sich nur auf die Durchführung von physischen Aktionen/Maßnahmen.

Situation: Was kann im Falle eines Hardware-Angriffs geschehen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Der häufigste Angriff auf Hardware bezieht sich nur auf nicht autorisierte physische Veränderungen.**
- **Physische Unfälle passieren häufiger, weil Menschen manchmal unverantwortliche Verhaltensweisen/Handlungen an den Tag legen.**
- **Angriffe auf Hardware können die persönlichen Daten und die physische Sicherheit des Hardwarebesitzers gefährden.**
- **Hardware-Angriffe stehen im Zusammenhang mit physischen Vorfällen und der Veränderung von Hardware.**

Situation: Welche Empfehlungen können bezüglich des Hardwareschutzes umgesetzt werden?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Halten Sie Ihre Hardware sauber und fern von Hitze- und Wasserquellen.
- Der Hardwareschutz sollte durch einen Softwareschutz ergänzt werden.
- Sie sollten den Kauf von Hardwarekomponenten aus risikoreichen Quellen/Ländern wegen möglicher unerwünschter Änderungen vermeiden.
- Personen können bei Bedarf spezielle Verfolgungssysteme und selbstzerstörende Geräte verwenden.

3.Wissen anwenden

Situation: Was ist die Bedeutung von Softwareschutz?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Kombination von Softwareschutz erfordert eine Kombination aus mehreren Techniken und Methoden.
- Softwareschutz ist meist reaktiv.
- Hardware- und Softwaresicherheit sollte eine Priorität sein, aber Softwareschutz muss häufiger durchgeführt werden.
- Softwareschutz ist wichtiger, weil die Menschen täglich mehr Software benutzen.

Situation: Was kann im Falle eines Software-Angriffs geschehen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Eine häufige Folge eines Software-Angriffs ist das Informationsleck.**
- **Eine weitere häufige Folge eines Software-Angriffs ist der unberechtigte Zugriff.**
- **Es kommt sehr häufig vor, dass bei einem Software-Angriff finanzielle Verluste entstehen.**
- **Gebrochene Authentisierung und mangelnder Schutz passieren oft gleichzeitig.**

Situation: Welche Empfehlungen können bezüglich Softwareschutz umgesetzt werden?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Man muss mehrere Methoden zum Schutz der Software implementieren und so oft wie möglich Leistungstests durchführen.**
- **Aktualisierte Firewalls, Antiviren- und Phishing-Filter sind Beispiele für den Schutz der Software.**
- **Da die Angriffe immer komplexer werden, müssen die Methoden zum Schutz der Anwendung aktualisiert werden.**
- **Da sich Software-Angriffe weiterentwickeln, sollten auch die Softwareschutzmaßnahmen aktualisiert werden.**