Dateiname: Cybersicherheitskurs I.mp4
Übersetzer: ScriptMe.io
Operator: Eingeladen
Datum der Transkription: Mar 31 2023

[00:00:03:02 - 00:00:55:20]
Sprecher 1: Hallo und willkommen zur interdisziplinären Cyber Training Unit 3. Für Manager lauten die Lernziele für diese Module: Was bedeutet es für ein kleines Unternehmen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu erreichen? Welche Regeln und Standards erwarten Ihre Regierung und Ihre Geschäftspartner von Ihnen? Und wir werden uns auch mit folgenden Themen befassen. Cybersecurity und Informationssicherheitsmanagement: Wie funktioniert Malware? Die wichtigsten Cyber-Bedrohungen, Arten von Angriffen, sichere Webserver, Senden und Empfangen von E-Mails und Asset Management. Zunächst einmal: Informationssicherheit für Manager - was ist Cybersicherheit?

[00:00:57:11 - 00:01:23:01]
Sprecher 1: Cybersicherheit ist der Schutz von Computern, Servern, mobilen Geräten, elektronischen Systemen, Netzwerken und Daten vor bösartigen Angriffen. Sie wird auch als Sicherheit der Informationstechnologie oder elektronische Informationssicherheit bezeichnet. Der Begriff findet in einer Vielzahl von Kontexten Anwendung, von Unternehmen bis hin zu mobilen Computern, und kann in ein paar allgemeine Kategorien unterteilt werden.

[00:01:30:18 - 00:01:51:03]
Sprecher 1: Es ist äußerst wichtig, dass die Schulungen zur Cybersicherheit für kleine und mittlere Unternehmen, Manager und Mitarbeiter konkret und interaktiv sowie praxisorientiert sind, da die kleinen und mittleren Unternehmen weder Zeit, Motivation noch Ressourcen haben, um sich mit diesem Thema zu befassen.

[00:01:52:07 - 00:02:19:03]
Sprecher 1: Warum? Es ist sehr wichtig, dass die Schulung für die Manager relevant und überschaubar ist, damit sie daran teilnehmen können. Daher ist dieses Modul auf der Grundlage dieses übergeordneten Ziels geplant. In diesem Modul werden wir uns ansehen, wie Sie die Cyber-Kill-Chain in Ihrer Cybersicherheitsstrategie effektiv nutzen können.

[00:02:20:14 - 00:02:43:16]
Sprecher 1: Analyse feiner Eindringversuche, wie man die Angriffe abwehren und stoppen kann, wie man die Datenkommunikation unterbricht, wie man die Wirksamkeit des Angriffs herabsetzt, reduziert und einschränkt, wie man die Angreifer täuscht und in die falsche Richtung lenkt, oder wie man die Reichweite des Angriffs eindämmt, verbirgt und begrenzt, so dass nur ein Teil des Unternehmens betroffen ist.

[00:02:50:20 - 00:03:18:06]

Sprecher 1: Feindliche, aufdringliche und absichtlich bösartige Malware versucht, in Computer, Computersysteme, Netzwerke, Tablets und mobile Geräte einzudringen, sie zu beschädigen oder zu deaktivieren. Oft übernimmt sie wie die menschliche Grippe die teilweise Kontrolle über den Betrieb eines Geräts und stört so die normale Funktion. Die Motive hinter Malware sind unterschiedlich. Bei Malware kann es darum gehen, aus Ihnen Geld zu machen.

[00:03:19:02 - 00:03:42:12]
Sprecher 1: Sie können Ihre Arbeit sabotieren, ein politisches Statement abgeben oder einfach nur damit prahlen. Obwohl Malware die physische Hardware von Systemen oder Netzwerkgeräten nicht beschädigen kann, kann sie dennoch Ihre Daten verschlüsseln oder löschen, die Funktionsweise von Computern verändern oder missbrauchen und Ihre Computeraktivitäten ohne Ihr Wissen oder Ihre Erlaubnis ausspionieren.

[00:03:53:17 - 00:04:49:00]
Sprecher 1: Beginnen wir also zunächst mit Malware. Was ist Malware? Nun, Malware steht für jedes Programm, dessen Funktion darin besteht, Software- oder Hardwareschäden auf einem Computer zu verursachen, wie z. B. Viren, Top-Cyber-Bedrohungen, Drive-by-Exploits können automatisch vorhandene Schwachstellen in der auf einem PC installierten Software ausnutzen, ohne dass eine Interaktion erfolgt. Sie konzentrieren sich fast ausschließlich darauf, legitime Websites zu kompromittieren. Schwachstellen im Browser, seinen Plugins oder dem Betriebssystem können ausgenutzt werden, um ohne Wissen des Benutzers Malware auf dem PC zu installieren.

[00:04:58:21 - 00:05:22:19]
Speaker 1: So now let's go to the next kind of malware, the worms. Worms are self replicating programs. They use the network of computers to send their own copies to other nodes computers in the network, managing to do this without the intervention of any user. Unlike a computer virus, a computer worm does not need to be attached to an existing program.

[00:05:23:23 - 00:05:52:00]
Speaker 1: As it causes damage to the network even just by taking up bandwidth, the Troyan, the Troyan presents itself in the form of legitimate programs, which in reality are created with the aim of stealing confidential confidential data or to allow unauthorized users or program access to the infected system.

[00:05:53:09 - 00:05:56:01]
Speaker 1: It constitutes the vast majority of infections, 80.

[00:05:56:10 - 00:06:02:19]
Speaker 2: Percent then we.

[00:06:02:22 - 00:06:20:24]
Speaker 1: Go into truckware as the name involves. Truckware are programs that use some

web browser vulnerabilities to send a server or people information about the sites accessed, the information searched, and the browsing habits of the user.

[00:06:22:08 - 00:06:51:07]
Speaker 1: Viruses aim to infect as many personal computers as possible, while spyware aims to spread across the Internet. Viruses usually have a dangerous payload, they want to cause damage to the infected computer, while spyware only slows down computer processes, adds pop ups and destabilizes the browser and has other annoying effects. And then we go into.

[00:06:52:07 - 00:07:36:14]
Speaker 1: Code injection, which is more complicated? Well, code injection occurs when an attacker can insert any data into an SQL query sent to a database. By injecting the syntax, the logic of the statement is modified so that it performs a different action. It is the most common vulnerability, the best SQL injection defense strategy. Is based on implementing strong input validation routines so that the attacker cannot enter data other than what the application needs, and then we go into.

[00:07:36:21 - 00:07:43:01]
Speaker 2: Spyware. Spyware.

[00:07:43:16 - 00:08:12:22]
Speaker 1: It is generally defined as a program. That takes advantage of the vulnerabilities of a system for the benefit of a third party. It can slow down your computer, make it vulnerable to virus infection, and collect confidential information such as usernames for various applications, passwords and credit bankaccount information. And then we go into key logger.

[00:08:15:14 - 00:09:09:10]
Speaker 1: A key logger basically is a small smart program that hackers place on your computer without you noticing. Here it can lie for several months or years and keep an eye on every single keystroke you make on the keyboard. All the data is sent to the hackers who can then use the different algorithms and tools to get the best out of your data. Overtime they find out different things about your behavior and not least. Where you use different passwords you have entered on the keyboard, it can be then used to take over your entire digital identity in a matter of minutes and then we go into adware.

[00:09:12:08 - 00:09:38:16]
Speaker 1: Hardware is a subcategory of spyware, and it is a program that advertises products or services. Often these ads appear even after the program has been uninstalled. Exploitation kits are automated software that assists less experienced attackers in compromising systems by exploiting client side vulnerabilities, particularly those in web browsers or applications that can be accessed by websites.

[00:09:40:00 - 00:09:48:23]
Speaker 1: Relies on drive by download attacks where malicious code is injected into compromised websites. It can exploit vulnerabilities in the browser or its.

[00:09:49:11 - 00:09:56:16]
Speaker 2: Plugins and there's.

[00:09:56:22 - 00:10:02:02]
Speaker 1: Many more like botnet, which represents a set of computers that are under control of an attacker.

[00:10:04:14 - 00:11:07:00]
Speaker 1: Denial of service, which is an attempt to affect the availability of computer systems, services or electronic communications. Here the target system is attacked by sending a very large number of illegitimate requests which consume its hardware or software resources, making it unavailable to legitimate users. Then we have rogueware or scareware, which is a type of threat that takes the form of fake software, a particular case of rogueware scareware. This fake security software that, once installed in the system, provides full security alerts and invites the user to purchase a special disinfection tool. And then there is ransomware, which is one of the most dangerous and aggressive forms of cybercrime. The hackers use a piece of extremely complex code to lock down the functionality of a computer or computer control system, the owner of the system. Is then contacted by the hacker with a demand for a ransom to reactivate the system or unlock information in the.

[00:11:07:03 - 00:11:14:02]
Speaker 2: System and then.

[00:11:14:06 - 00:11:22:19]
Speaker 1: We go into types of attacks. You have targeted attacks which basically they target the specific person or organization.

[00:11:25:21 - 00:11:48:10]
Speaker 1: Some of them aim to collect either personal or confidential data or compromise target computer system and generally it has a phase in which the attacker informs himself through various techniques like social engineering about the targeted i t system and then triggers the attack often his actions appear legitimate because they appear to be coming from a trustworthy person.

[00:11:51:05 - 00:12:46:09]
Speaker 1: Another one is theft losses, physical destruction, which is due to the increased mobility offered by laptops, smartphones or tablets. This type of threat is about to become a major one. It's basically consistent. Data backup and content encryption can be a solution to limit actual data loss or disclosure of confidential data to outsiders. And then there is of

course identity theft. Which is a real threat in an increasingly online environment. People can access credentials or personal data and that is the target of attackers today. Once they possess your credential and personal data, the attacker can carry out fraudulent transactions, especially financial, or obtain other confidential data. Another type of attack is information leak, which can be intentional or unintentional disclosure information to an authorized.

[00:12:47:15 - 00:13:11:08]
Speaker 1: Unauthorized person information such as geolocation and phone book contacts can easily fall in the hands of attackers and be used for fraudulent purposes. Types of attacks we have search engine manipulation.

[00:13:12:24 - 00:13:37:03]
Speaker 1: This one is about manipulating search engines to display search results that contain references to malicious websites. Thus, an infected web page redirects the user to malicious sites and if the victims access the respective sites they invest, they invest their computers with malware. There's also about fake digital certificates which are used by attackers to digitally sign resources.

[00:13:38:21 - 00:14:05:05]
Speaker 1: Used in various cyber attacks in order to pass undetectable to the end user. They're often used to sign malicious web applications such as E banking or ecommerce, which use the HTTPS protocol. They can be created or stolen by exploiting vulnerabilities in PKI, public key infrastructure system of certification authorities that issue digital certificates for secure websites.

[00:14:10:19 - 00:14:32:19]
Speaker 1: Then we can go into secure web servers. SSL, the protocol that implements public key encryption is called SSL secure socket layer developed by Netscape. This protocol is used by browser and web servers to transmit data securely.

[00:14:34:02 - 00:15:00:02]
Speaker 1: So it so it was created to be used by the HTTP protocol. Connecting to a secure web server is done by mentioning the HTTPS protocol instead of HTTP in the URL. That is, access to the secure Web page is indicated by the protocol and not the name of the server. A secure Web server offers secure transfer information. The data transmitted between the server and the navigator cannot be decrypted in case of their interception.

[00:15:01:23 - 00:15:34:22]
Speaker 1: Server identification. If the web server has received a certificate from a certification authority security checklist, well, it's what is important to do to secure your digital devices. Firewalls. Well start by securing your outer parameters by making sure your points firewalls work. It sounds basic but it is also the very basics that you have to start.

[00:15:36:02 - 00:16:00:21]

Speaker 1: There are typically three to four types of firewalls on your network. There's a firewall on your operating system, which can be Android, iOS, Windows, etcetera. There can be a firewall on your antivirus security program. There can be a firewall on your Internet router, and there can be a firewall on your ASA box or intelligence switch, which typically is only had by larger companies.

[00:16:04:07 - 00:16:30:18]
Speaker 1: Another thing that we suggest that you do is backup. Backup should really be at the top of the list like it shouldn't be news. Backup can save you from having to pay a ransom to have your data unlocked. However, make no mistake about the size of the company. Most of the attacks with this type of malware are aimed at small businesses and individuals.

[00:16:35:18 - 00:16:57:07]
Speaker 1: And then we go of course into rules for browsing. Well, how can you be more safe when you browse? Make sure that you use the latest browser version. Orient yourself towards other types of browser, for example Google Chrome, Opera, Fireworks, Safari, etc. Especially when accessing potentially unsafe web pages.

[00:16:58:23 - 00:17:26:16]
Speaker 1: Most malware affects microsoft internet explorer used by over fifty percent of the users check the real destination of the links by passing the mouse cursor over it and viewing the real address in the lower left part of the browser be careful what plugins you install often they come with malicious software do not click on links in pop up windows check for https dot.

[00:17:28:14 - 00:17:56:05]
Speaker 1: At the beginning of the web address, before entering personal information and regarding making an online purchase, greater attention must be paid to the security level of the page. If one opts for online payment with the bank card also about how to safely send and receive an e-mail, well, of course, avoid sending or receiving sensitive information by e-mail.

[00:17:58:10 - 00:18:23:18]
Speaker 1: Avoid social engineering or phishing attempts look for an email provider that actually offers strong r and t spam filtering do not respond to spam and avoid cascade or pyramid emails do not respond do not use the same name for your personal and work email account the use use of distinct names for this accounts reduces the risk of them being the target of a computer attack.

[00:18:25:06 - 00:18:53:19]
Speaker 1: Avoid storing critical information in personal e-mail accounts or in other networks outside the institution company where you work. Arguing that you don't care about privacy because you have nothing to hide is like arguing that you don't care about free speech because you have nothing to say, while many people may still subscribe to the mindset that

they have nothing to be concerned about.

[00:18:54:19 - 00:20:14:04]
Speaker 1: If they have nothing to hide, the reality is that there is plenty to be concerned about. And there are plenty of concrete reasons for people to encrypt their e-mail communications and protect their privacy. This is true whether you're an investigative journalist, dissident, whistleblower, or just an ordinary average citizen. And why will anyone need a secure e-mail? Well. Have you ever sent sensitive personal information and e-mail and thought, well, I sure hope this e-mail doesn't somehow end up in the wrong hands. This is a truly disconcerting fault because if someone other than the intended recipients get their hands on the e-mail, especially that someone happens to be a cyber criminal, the results could potentially be catastrophic. Sending an e-mail containing sensitive personal data. Like your medical information, financial account information, Social Security number, address, or phone number can be extremely risky because cyber criminals need only a minimal amount of personal data to exact maximum harm. With access to sensitive personal data like this, cyber criminals can compromise your online profiles, drain your bank accounts, or even steal your identity.

[00:20:16:01 - 00:20:40:12]
Speaker 1: Sending an encrypted e-mail preserve your preserves your privacy and effectively makes it impossible for other entities to Snoop on your secure e-mail communications. This is especially important for those whose job responsibilities require complete confidentiality in their communications, but it's also vital for anyone who generally doesn't want the government trampling on their privacy rights.

[00:20:45:21 - 00:21:43:09]
Speaker 1: This is why sending emails is critical, particularly if the e-mail you're sending contains sensitive personal information. Now that you know the reasons why you'd want to send a secure e-mail, we're guessing you'll probably want to know how to actually do it well, there are a couple of ways to go about doing so, each with certain inherent advantages and disadvantages, but the bottom line is. That if you're going to send a secure e-mail, then your e-mail message will need to be encrypted. When you encrypt an e-mail message, you're essentially scrambling the contents of that message and making it impossible for anyone without the encryption key to unscramble the message. For example, if you want to send a secure e-mail on Gmail, you will first need to enable S MIME encryption by signing into Gmail using a G Suite administrator account.

[00:21:44:20 - 00:22:08:18]
Speaker 1: G Suite accounts are primarily for business purposes, but you could theoretically set up an account for your personal use. The other issue with this is that the recipients you are emailing will also need to have S MIME encryption activated in order for this to work. You can also use a dedicator dedicated e-mail provider.

[00:22:12:11 - 00:22:38:19]
Speaker 1: You can however bypass these issues by installing a free third party to like mail velop to encrypt your emails with ease. Mail Velop works with many of the most popular e-

mail services like Gmail, Yahoo, Outlook, Hotmail, and GMX. But again, the recipients of your encrypted e-mail message will also need to be using similar PGP Open PGP software to decrypt the e-mail and read the contents.

[00:22:40:10 - 00:23:08:15]
Speaker 1: With the secure e-mail provider like ProtonMail, you'll be able to send secure encrypted emails to others regardless of whether they use the same e-mail provider that you use, and your recipients will also be able to respond securely. Many secure e-mail providers implement open PGP encryption to secure users emails, and will also allow users to easily send and receive secure encrypted emails with others who have open PGP encryption enabled with their e-mail clients.

[00:23:10:05 - 00:23:35:11]
Speaker 1: If your recipient does not have PGP enabled, then you'll be able to send an e-mail secure list to that recipient that can only be opened using a shared secret. Basically, when you use the secure e-mail provider, you'll be able to easily protect sensitive messages by encrypting them all on a platform that is typically as simple to use as the big name e-mail providers like Gmail, Yahoo, or Outlook.

[00:23:36:21 - 00:24:02:02]
Speaker 1: But unlike those big name providers, a secure e-mail provider won't annoy you with my advertisements or monitor your emails since it can't even access them thanks to the end to end encryption. The downside is that in order to access a secure e-mail providers full slate of features, expanded storage or unrestricted messaging, you'll need to pay. Many of the best secure e-mail providers do, however offer a free.

[00:24:03:06 - 00:24:22:10]
Speaker 1: Here with certain limitations that will allow you to send and receive secure emails for free. If you're only going to be sending a limited number of secure emails, then a free option will certainly be a viable solution. But if you're planning on conducting the majority of your e-mail correspondence in a secure manner, then purchasing a premium subscription will be.

[00:24:23:01 - 00:24:29:15]
Speaker 2: Necessary when you.

[00:24:29:20 - 00:24:30:12]
Speaker 1: Receive an e-mail.

[00:24:31:24 - 00:25:27:20]
Speaker 1: You have to be paying attention to the fact that the identity of the sender is not guaranteed. You should check the relationships between the sender and the content of the message. Do not open attachments coming from unknown persons or associated with legitimate accounts, but with messages with suspicious subject and content. They may

contain malicious software such as worms, troyans, spyware. Hardware, etc. If it is absolutely necessary to open an attachment, even from legitimate emails, it must first be downloaded and scanned with the installed antivirus solution and then opened with the associated application. In the case of emails containing links, do not directly access that link in the body of the message. Possibly that link can be copied and opened from another browser tab.

[00:25:29:10 - 00:25:58:01]
Speaker 1: Do not respond to emails containing requests for personal or confidential data like pin code bank card number and then we have to go into how to make your your email stronger so i'll be a password so what are the methods for making strong passwords well there is the phonetic method i know for sure i have a blu ray dvd or the first letter method.

[00:25:59:19 - 00:27:26:01]
Speaker 1: Or the substitution method. Usually vowels the reverse and substitution method, the upper and lower case number and symbol and substitution method. Customization of methods according to websites in order to create a personal password generation system measures you can use the CAPTCHA system access timing after number of failed accesses, use unique ID's and passwords and do not communicate them. To other users, the length of the password and its complexity must be chosen so that it is difficult to guess but easy to remember periodic changes of passwords, at least at an interval of one to three months using different passwords for different applications. Use multiple identification methods like pin, fingerprint, alert messages, etc. And avoid using similar passwords at home and at work. Do not use. The name, your name, someone else in your family, or your favorite animal. Do not use elements of your address, building name, St. Country, the name of your the institution, the project, the phone number, registration number, the name of the favorite star or character dictionary words, or the name of the account for which you set the password. Thank you for your attention and see you at the next slides.

[00:27:27:02 - 00:27:29:18]
Speaker 2: Show Vijay Prakash Kannada sung.