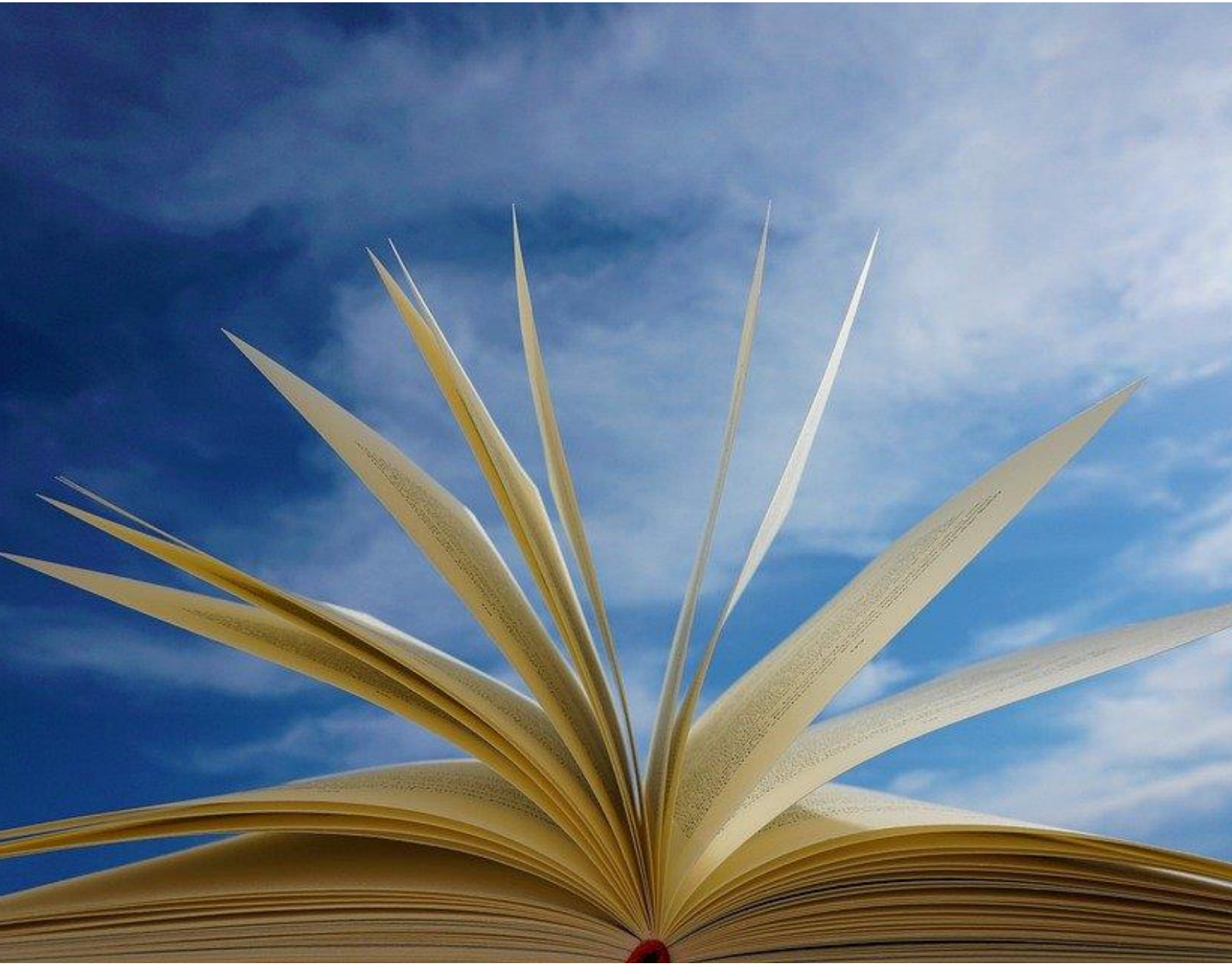

Glossary / Glossar/ Glosariusz / Žodynas / Glossario

I

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

TeBeISi

This document was produced as part of the ERASMUS+ project "Partial certification in the professional field of information security - TeBeiSi", Project ID: 2018-1-EN02-KA202-005218

Funded by the
Erasmus+ Programme
of the European Union

1. Introduction

Indroduction

This multilingual glossary defines xx key terms used in the TeBeISi project. This glossary is published in English, German, Polish, Lithuanian and Italian. Every term is provided with a description and an information to the source which it is based on.

Einführung

Dieses mehrsprachige Glossar definiert xx Schlüsselbegriffe, die im TeBeISi Projekt verwendet werden. Dieses Glossar ist auf Englisch, Deutsch, Polnisch, Litauisch und Italienisch veröffentlicht. Jeder Begriff wird mit einer Beschreibung und einer Information zu der Quelle versehen, auf der er basiert.

Wprowadzenie

Ten wielojęzyczny glosariusz definiuje kluczowe terminy xx używane w projekcie TeBeISi. Glosariusz ten jest publikowany w języku angielskim, niemieckim, polskim, litewskim i włoskim. Każdy termin jest opatrzony opisem i informacją o źródle, na którym jest oparty.

Lit: Įvadas

Šis daugiakalbis žodynas apibrėžia xx pagrindinius terminus, naudojamus „TeBeISi“ projekte. Šis žodynas išleidžiamas anglų, vokiečių, lenkų, lietuvių ir italų kalbomis. Kiekvienam terminui pateikiamas aprašymas ir informacijos šaltinis, kuriuo jis grindžiamas.

Introduzione

Questo glossario multilingue definisce xx termini chiave utilizzati nel progetto TeBeISi. Questo glossario è pubblicato in inglese, tedesco, polacco, lituano e italiano. Ogni termine viene fornito con una descrizione e informazioni sulla fonte su cui si basa.

2. Alphabetical index for each term

3. Glossary

account

An account is a user account with a service provider that requires access authorization. This includes, for example, retrieving and sending e-mails, participating in discussion forums or conducting online banking transactions. Once the user account has been created, authentication as a user is usually performed by entering a user name and password.

Source: Glossary of BSI

DE Account/ Benutzerkonto

Ein Account ist ein Benutzerkonto bei einem Dienstanbieter, das eine Zugangsberechtigung erfordert. Dazu gehören z.B. das Abrufen und Versenden von E-Mails, die Teilnahme in Diskussionsforen oder die Abwicklung von Online-Bankgeschäften. Nach dem Anlegen des Benutzerkontos erfolgt die Authentifizierung als Nutzer normalerweise durch die Angabe eines Nutzernamens und eines Passworts.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL konto

Konto to konto użytkownika u usługodawcy, które wymaga autoryzacji dostępu. Dotyczy to na przykład pobierania i wysyłania wiadomości e-mail, uczestniczenia w forach dyskusyjnych lub przeprowadzania transakcji bankowych online. Po utworzeniu konta użytkownika, uwierzytelnienie jako użytkownik odbywa się zazwyczaj poprzez wprowadzenie nazwy użytkownika i hasła.

Źródło: Słownikf BSI

LIT paskyra

Paskyra yra paslaugų teikėjo vartotojo paskyra, kuriai reikalingas prieigos leidimas. Tai apima, pavyzdžiui, elektroninių laiškų gavimą ir siuntimą, dalyvavimą diskusijų forumuose ar internetinės bankininkystės operacijų atlikimą. Sukūrus vartotojo paskyrą, autentifikavimas paprastai atliekamas įvedant vartotojo vardą ir slaptažodį.

šaltinis:

IT conto

Un account è un conto utente con un fornitore di servizi che richiede un'autorizzazione di accesso. Questo include, per esempio, il recupero e l'invio di e-mail, la partecipazione a forum di discussione o lo svolgimento di transazioni bancarie online. Una volta che l'account è stato creato, l'autenticazione come utente viene solitamente eseguita inserendo un nome utente e una password.

Fonte: adattato da xy

administrator

A person who is responsible for setting up, operating, monitoring, and/or maintaining an IT system or network.

Source: VDS 10000

DE Administrator

Person, die für Einrichtung, Betrieb, Überwachung und/oder Wartung eines IT-Systems oder Netzwerks zuständig ist.

Quelle: VDS 10000

POL adminitrator

Osoba, która jest odpowiedzialna za konfigurację, obsługę, monitorowanie i/lub konserwację systemu informatycznego lub sieci.

Źródło: VDS 10000

LIT administratorius

Asmuo, atsakingas už IT sistemos ar tinklo sukūrimą, valdymą, stebėjimą ir (arba) priežiūrą.

šaltinis: VDS 10000

IT amministratore

Una persona che è responsabile dell'impostazione, del funzionamento, del monitoraggio e/o della manutenzione di un sistema o di una rete IT.

Fonte: VDS 10000

algorithm

An algorithm defines a course of action for solving a problem or a specific type of problem. In computer science: processing instruction that is formulated so unambiguously that a machine-executable program can reproduce it.

Source: Glossary of BSI

DE Algorithmus

Definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen. In der Informatik: Verarbeitungsvorschrift, die so eindeutig formuliert ist, dass sie durch ein maschinell ausführbares Programm wiedergegeben werden kann.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL algorytm

Algorytm definiuje sposób postępowania przy rozwiązywaniu problemu lub określonego typu problemu. W informatyce: instrukcja przetwarzania, która jest sformułowana tak jednoznacznie, że program wykonywany maszynowo może ją odtworzyć.

Źródło: Słownikf BSI

LIT algorithmas

Algoritmas apibrėžia problemos ar tam tikros rūšies problemos sprendimo būdą. Kompiuterių moksle: apdorojimo instrukcija, kuri yra suformuluota taip vienareikšmiškai, kad mašina vykdoma programa gali ją atkurti.

šaltinis:

IT algoritmo

Un algoritmo definisce una linea d'azione per risolvere un problema o un tipo specifico di problema. In informatica: istruzione di elaborazione che è formulata in modo così univoco che un programma eseguibile dalla macchina può riprodurla.

Fonte: Glossario di BSI

antivirus program

An antivirus program checks new files (for example, attachments to e-mails) and the entire computer for malware. To do this, it primarily compares the data on the computer with the "fingerprints" of known malware.

Source: Glossary of BSI

DE Virenschutzprogramm

Ein Virenschutzprogramm überprüft neue Dateien (z.B. Anhänge von E-Mails) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den "Fingerabdrücken" bekannter Schadprogramme.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL program antywirusowy

Program antywirusowy sprawdza nowe pliki (na przykład załączniki do wiadomości e-mail) i cały komputer pod kątem obecności złośliwego oprogramowania. W tym celu przede wszystkim porównuje dane na komputerze z "odciskami palców" znanego złośliwego oprogramowania.

Źródło: Słownikf BSI

LIT antivirusinė programa

Antivirusinė programa tikrina naujus failus (pvz., priedus prie el. laiškų) ir visą kompiuterį, ar nėra kenkėjiškų programų. Norėdami tai padaryti, ji pirmiausia lygina kompiuteryje esančius duomenis su žinomų kenkėjiškų programų „pirštų atspaudais“.

šaltinis: BSI žodynas

IT programma antivirus

Un programma antivirus controlla i nuovi file (per esempio, gli allegati alle e-mail) e l'intero computer alla ricerca di malware. Per fare questo, confronta principalmente i dati sul computer con le "impronte digitali" di malware conosciuti.

Fonte: Glossario di BSI

applied threat

Threat that specifically affects an object via a vulnerability. A threat thus only becomes a danger to an object through an existing vulnerability.

Source: Glossary of BSI

DE Gefährdung

Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL stosowane zagrożenie

Zagrożenie, które w szczególny sposób wpływa na obiekt poprzez lukę w zabezpieczeniach. Zagrożenie staje się więc niebezpieczeństwem dla obiektu tylko poprzez istniejącą lukę.

Źródło: Słownikf BSI

LIT pritaikyta grėsmė

Grėsmė, kuri konkrečiai veikia objektą per pažeidžiamumą. Taigi grėsmė tampa pavojumi objektui tik per esamą pažeidžiamumą.

šaltinis:

IT minaccia applicata

Minaccia che colpisce specificamente un oggetto tramite una vulnerabilità. Una minaccia diventa quindi un pericolo per un oggetto solo attraverso una vulnerabilità esistente.

Fonte: Glossario di BSI

attachment

Files attached to an e-mail (documents, images, videos, music files, etc.).

Source: Glossary of BSI

DE Anhang

An eine E-Mail angehängte Datei (Dokumente, Bilder, Videos, Musikdateien, etc.).

Quelle: Glossar der Cyber-Sicherheit - BSI

POL załącznik

Pliki dołączone do wiadomości e-mail (dokumenty, obrazy, wideo, pliki muzyczne itp.)

Źródło: Słownikf BSI

LIT prisegtukas

Prie el. laiško pridedami failai (dokumentai, vaizdai, vaizdo įrašai, muzikos failai ir kt.)

šaltinis: BSI žodynas

IT allegato

File allegati a una e-mail (documenti, immagini, video, file musicali, ecc.)

Fonte: Glossario di BSI

attack

An attack is an intentional endangerment, namely an unwanted or unauthorized act to gain advantages or harm a third party. Attackers can also act on behalf of third parties who want to gain benefits.

Source: Glossary of BSI

DE Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL atak

Atak jest celowym zagrożeniem, czyli niechcianym lub nieuprawnionym działaniem mającym na celu uzyskanie korzyści lub zaszkodzenie stronie trzeciej. Atakujący mogą również działać w imieniu osób trzecich, które chcą uzyskać korzyści.

Źródło: Słownikf BSI

LIT ataka

Ataka yra tyčinis pavojus, t.y. nepageidaujamas ar neteisėtas veiksmas, siekiant naudos ar žalos trečiajai šaliai. Užpuolikai taip pat gali veikti trečiųjų šalių, norinčių gauti naudos, vardu.

šaltinis: BSI žodynas

IT attacco

Un attacco è un pericolo intenzionale, cioè un atto indesiderato o non autorizzato per ottenere vantaggi o danneggiare una terza parte. Gli aggressori possono anche agire per conto di terzi che vogliono ottenere vantaggi.

Fonte: Glossario di BSI

authentication

Authentication is a way to ascertain that a user is who they claim to be. This is usually performed by presenting one or more challenges to the user.

Source: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods

DE Authentisierung

Bei der Authentisierung legt eine Person einen Nachweis über ihre Identität vor, um ihn von einem System überprüfen zu lassen. Dies kann u.a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z.B. durch kryptographische Signaturen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL uwierzytelnianie

Uwierzytelnianie jest sposobem na upewnienie się, że użytkownik jest tym, za kogo się podaje. Zazwyczaj odbywa się to poprzez przedstawienie użytkownikowi jednego lub więcej wyzwań.

Źródło: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods

LIT autentifikavimas

Autentifikavimas yra būdas įsitikinti, kad vartotojas yra tas, kuo jis teigia. Paprastai tai atliekama pateikiant vartotojui vieną ar kelis iššūkius.

šaltinis: BSI žodynas

IT autenticazione

L'autenticazione è un modo per accertare che un utente sia chi dice di essere. Questo viene solitamente eseguito presentando una o più sfide all'utente.

Fonte: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods

authenticity

The term authenticity is used to describe the property that ensures that a communication partner is actually who he claims to be. Authentic information confirms that the specified source created it. The term is used not only when checking the identity of people but also for IT components or applications.

Source: Glossary of BSI

DE Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL Authentizität

Termin wiarygodność jest używany do opisania właściwości, która zapewnia, że partner komunikacyjny jest tym, za kogo się podaje. Autentyczne informacje potwierdzają, że określone źródło je stworzyło. Termin ten jest używany nie tylko przy sprawdzaniu tożsamości osób, ale także komponentów IT lub aplikacji.

Źródło: Słownikf BSI

LIT autentiškumas

Sąvoka autentiškumas naudojamas apibūdinti nuosavybę, užtikrinantį, kad bendravimo partneris iš tikrųjų yra toks, koks jis teigia esąs. Autentiška informacija patvirtina, kad nurodytas šaltinis ją sukūrė. Terminas naudojamas ne tik tikrinant žmonių tapatybę, bet ir IT komponentus ar programas.

šaltinis: BSI žodynas

IT autenticità

Il termine autenticità è usato per descrivere la proprietà che assicura che un partner di comunicazione sia effettivamente chi dice di essere. L'informazione autentica conferma che la fonte specificata l'ha creata. Il termine è usato non solo quando si controlla l'identità delle persone, ma anche per i componenti o le applicazioni IT.

Fonte: Glossario di BSI

authorization

During an authorization, the rights granted to a person on a system are released for an already successfully authenticated person.

Source: Glossary of BSI

DE Autorisierung

Bei der Autorisierung werden für eine bereits erfolgreich authentifizierte Person die ihr auf einem System eingeräumten Rechte freigeschaltet.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL Autorisierung

Podczas autoryzacji uprawnienia przyznane danej osobie w systemie są ujawniane osobie, która została już pomyślnie uwierzytelniona.

Źródło: Słownikf BSI

LIT leidimas

Įgaliojimo metu sistemoje jau esančiam asmeniui suteiktos teisės leidžiamos jau sėkmingai patvirtintam asmeniui.

šaltinis:

IT autenticità

Il termine autenticità è usato per descrivere la proprietà che assicura che un partner di comunicazione sia effettivamente chi dice di essere. L'informazione autentica conferma che la fonte specificata l'ha creata. Il termine è usato non solo quando si controlla l'identità delle persone, ma anche per i componenti o le applicazioni IT.

Fonte: Glossario di BSI

backdoor

Backdoors are malicious programs that are used to keep open an unauthorized access to an IT system that allows an unnoticed break-in into the system with the broadest possible access rights, for example to hide attack traces.

Source: Glossary of BSI

DE Hintertür

Hintertüren sind Schadprogramme, die dazu dienen, einen unbefugten Zugang zu einem IT-System offen zu halten, der einen unbemerkten Einbruch in das System ermöglicht und dabei möglichst weitgehende Zugriffsrechte besitzt, bspw. um Angriffsspuren zu verstecken.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL backdoor

Backdoor to złośliwe programy, które służą do otwarcia nieautoryzowanego dostępu do systemu informatycznego, umożliwiającego niezauważalne włamanie się do systemu z jak najszerszymi prawami dostępu, np. w celu ukrycia śladów ataku.

Źródło: Słownikf BSI

LIT galinės durys

Užpakalinės durys yra kenkėjiškos programos, naudojamos neleistinai prieigai prie IT sistemos, kuri leidžia nepastebimai įsilaužti į sistemą ir suteikti kuo platesnes prieigos teises, pavyzdžiui, paslėpti atakų pėdsakus.

šaltinis: BSI žodynas

IT backdoor

Le backdoor sono programmi maligni che vengono utilizzati per tenere aperto un accesso non autorizzato a un sistema informatico che permette un'intrusione inosservata nel sistema con i diritti di accesso più ampi possibili, per esempio per nascondere le tracce di un attacco.

Fonte: Glossario di BSI

backup

Backup of data to protect against data loss. Copies of existing data sets are created in the process.

Source: Glossary of BSI

DE Datensicherung

Sicherung der Daten zum Schutz vor Datenverlust. Dabei werden Kopien von vorhandenen Datenbeständen erstellt.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL backup

Tworzenie kopii zapasowych danych w celu zabezpieczenia przed ich utratą. W procesie tym tworzone są kopie istniejących zbiorów danych.

Źródło: Słownikf BSI

LIT rezervinė kopija

Atsarginė duomenų kopija, skirta apsaugoti nuo duomenų praradimo. Proceso metu sukuriamos esamų duomenų rinkinių kopijos.

šaltinis: BSI žodynas

IT backup

Backup dei dati per proteggere dalla perdita di dati. Nel processo vengono create copie dei set di dati esistenti.

Fonte: Glossario di BSI

basic values of information security

Basic IT protection considers the three basic values of information security: confidentiality, availability and integrity. Of course, every user is free to consider other basic values when determining the need for protection if this is helpful in his or her individual use case. Other generic generic terms of information security are, for example: authenticity, bindingness, reliability and non-repudiation.

Source: Glossary of BSI

DE Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität. Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel: Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL podstawowe zasady bezpieczeństwa informacji

Podstawowa ochrona informatyczna uwzględnia trzy podstawowe wartości bezpieczeństwa informacji: poufność, dostępność i integralność. Oczywiście, każdy użytkownik może uwzględnić inne podstawowe wartości przy określaniu potrzeby ochrony, jeśli jest to pomocne w jego indywidualnym zastosowaniu. Innymi ogólnymi pojęciami z zakresu bezpieczeństwa informacji są na przykład: autentyczność, wiążący charakter, wiarygodność i niezaprzeczalność.

Źródło: Słownikf BSI

LIT pagrindines informacijos saugumo vertybes

Pagrindinė IT apsauga apima tris pagrindines informacijos saugumo vertybes: konfidencialumą, prieinamumą ir vientisumą. Žinoma, kiekvienas vartotojas, nustatydamas apsaugos poreikį, gali laisvai atsižvelgti į kitas pagrindines vertybes, jei tai naudinga jo asmeniniam naudojimui. Kitos bendros bendros informacijos saugumo sąlygos yra, pavyzdžiui: autentiškumas, privalomumas, patikimumas ir neatsisakymas.

šaltinis: BSI žodynas

IT valori di base della sicurezza delle informazioni

La protezione informatica di base considera i tre valori fondamentali della sicurezza delle informazioni: riservatezza, disponibilità e integrità. Naturalmente, ogni utente è libero di considerare altri valori di base nel determinare il bisogno di protezione se questo è utile nel suo caso d'uso individuale. Altri termini generici della sicurezza delle informazioni sono, per esempio: autenticità, vincolatività, affidabilità e non ripudio.

Fonte: Glossario di BSI

boot viruses

Viruses that are executed when the operating system is started (booted) and then remain in memory. They can infect the boot sectors of hard disks and floppy disks. They are usually transmitted by booting from an infected boot diskette (or CD-ROM).

Source: Glossary of BSI

DE Bootviren

Viren, die bereits beim Starten (Booten) des Betriebssystems ausgeführt werden und anschließend im Arbeitsspeicher verbleiben. Sie können die Boot-Sektoren von Festplatten und Disketten befallen. Übertragen werden sie meist dadurch, dass von einer infizierten Startdiskette (oder CD-ROM) gebootet wird.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL wirusy startowe

Wirusy, które są uruchamiane w momencie startu systemu operacyjnego i pozostają w pamięci. Mogą one infekować sektory startowe dysków twardych i napędów dyskietek. Zazwyczaj są one przenoszone przez uruchomienie systemu z zainfekowanej dyskietki startowej (lub CD-ROM).

Źródło: Słownikf BSI

LIT įkrovos virusai

Virusai, kurie paleidžiami paleidus operacinę sistemą (paleidžiant) ir lieka atmintyje. Jie gali užkrėsti standžiųjų diskų ir diskelių įkrovos sektorius. Paprastai jie perduodami paleidžiant iš užkrėsto įkrovos disko (arba kompaktinio disko).

šaltinis: BSI žodynas

IT virus d'avvio

Virus che vengono eseguiti quando il sistema operativo viene avviato (booted) e poi rimangono in memoria. Possono infettare i settori di avvio dei dischi rigidi e dei floppy disk. Di solito vengono trasmessi avviando da un dischetto di avvio (o CD-ROM) infetto.

Fonte: Glossario di BSI

bot

The term bot is derived from the English term "robot". Bots are computer programs that, once activated, operate automatically on the Internet without human intervention. A group of bots forming a communication network is known as a botnet.

Source: Glossary of BSI

DE Bot

Der Begriff Bot ist vom englischen Begriff "robot" (dt. Roboter) abgeleitet. Bots sind Computerprogramme, die nach ihrer Aktivierung ohne menschliches Zutun automatisiert im Internet agieren. Einen Zusammenschluss von Bots zu einem Kommunikationsverbund bezeichnet man als Botnetz.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL bot

Termin bot pochodzi od angielskiego terminu "robot". Boty to programy komputerowe, które po uruchomieniu działają automatycznie w Internecie bez ingerencji człowieka. Grupa botów tworząca sieć komunikacyjną nazywana jest botnetem.

Źródło: Słowniczek BSI

LIT botas

Terminas „bot“ yra kilęs iš angliško termino „robotas“. Robotai yra kompiuterinės programos, kurios, suaktyvintos, automatiškai veikia internete be žmogaus įsikišimo. Ryšių tinklą sudaranti robotų grupė yra žinoma kaip botnetas.

šaltinis: BSI žodynas

IT bot

Il termine bot deriva dal termine inglese "robot". I bot sono programmi per computer che, una volta attivati, operano automaticamente su Internet senza intervento umano. Un gruppo di bot che forma una rete di comunicazione è noto come botnet.

Fonte: Glossario di BSI

Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) is a strategy by institutions to encourage their employees to use their private devices for business purposes or even create financial incentives. The special feature of BYOD is that the end devices may be subsidized by the organization but are the property of the employees.

Source: Glossary of BSI

DE Bring Your Own Device (BYOD)

Bei BYOD (Bring Your Own Device) handelt es sich um Strategien von Institutionen, ihre Mitarbeiter zur dienstlichen Nutzung ihrer privaten Geräte zu ermutigen oder sogar finanzielle Anreize hierfür zu schaffen. Die Besonderheit an BYOD ist, dass die Endgeräte zwar unter Umständen durch die Institution subventioniert werden aber Eigentum der Mitarbeiter sind.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL bot

Termin bot pochodzi od angielskiego terminu "robot". Boty to programy komputerowe, które po uruchomieniu działają automatycznie w Internecie bez ingerencji człowieka. Grupa botów tworząca sieć komunikacyjną nazywana jest botnetem.

Źródło: Słownikf BSI

LIT Atsineškite savo įrenginį (BYOD)

BYOD (Bring Your Own Device) yra institucijų strategija, skatinanti savo darbuotojus naudoti savo asmeninius įrenginius verslo tikslais ar net sukurti finansinių paskatų. Ypatingas BYOD bruožas yra tas, kad galutinius įrenginius gali subsidijuoti organizacija, tačiau jie yra darbuotojų nuosavybė.

šaltinis: BSI žodynas

IT Porta il tuo dispositivo personale (BYOD)

BYOD (Bring Your Own Device) è una strategia delle istituzioni per incoraggiare i loro dipendenti a utilizzare i loro dispositivi privati per scopi aziendali o anche creare incentivi finanziari. La particolarità del BYOD è che i dispositivi finali possono essere sovvenzionati dall'organizzazione ma sono di proprietà dei dipendenti.

Fonte: Glossario di BSI

business continuity management

Business continuity management (BCM) refers to all organizational, technical and personnel measures that serve to continue the core business of an authority or a company after an emergency or security incident. Furthermore, BCM supports the successful continuation of business processes in the event of prolonged outages or disruptions.

Source: Glossary of BSI

DE Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL zarządzanie ciągłością biznesu

Zarządzanie ciągłością biznesową (BCM) odnosi się do wszystkich środków organizacyjnych, technicznych i personalnych, które służą do kontynuowania podstawowej działalności organu lub przedsiębiorstwa po wystąpieniu sytuacji awaryjnej lub incydentu bezpieczeństwa. Ponadto BCM wspiera pomyślną kontynuację procesów biznesowych w przypadku przedłużających się przestojów lub zakłóceń.

Źródło: Słownikf BSI

LIT veiklos tęstinumo valdymas

Veiklos tęstinumo valdymas (BCM) reiškia visas organizacines, technines ir personalo priemones, kuriomis siekiama tęsti pagrindinę institucijos ar įmonės veiklą po avarijos ar saugumo incidento. Be to, BCM palaiko sėkmingą verslo procesų tęstinumą ilgalaikių pertraukų ar sutrikimų atveju.

šaltinis: BSI žodynas

IT gestione della continuità aziendale

Il Business continuity management (BCM) si riferisce a tutte le misure organizzative, tecniche e di personale che servono a continuare il core business di un'autorità o di un'azienda dopo un'emergenza o un incidente di sicurezza. Inoltre, il BCM supporta la continuazione di successo dei processi di business in caso di interruzioni o disservizi prolungati.

Fonte: Glossario di BSI

The identification of critical business processes, and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes.

Source: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

DE BIA (Business Impact Analyse)

Eine Business Impact Analyse (Folgeschädenabschätzung) ist eine Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL analiza skutków biznesowych

Identyfikacja krytycznych procesów biznesowych oraz potencjalnych szkód lub strat, jakie mogą być spowodowane w organizacji w wyniku zakłócenia tych procesów.

Źródło: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

LIT poveikio verslui analizė

Kritinių verslo procesų nustatymas ir galima žala ar nuostoliai, kuriuos organizacija gali patirti dėl šių procesų sutrikimo.

šaltinis: BSI žodynas

IT analisi dell'impatto aziendale

L'identificazione dei processi aziendali critici e i potenziali danni o perdite che possono essere causati all'organizzazione a causa di un'interruzione di tali processi.

Fonte: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

certificate

The term certificate is used in information security in various areas with different meanings. A distinction must be made between ISO 27001 certificates (the ISO 27001 standard enables certification of information security management) and ISO 27001 certificates based on basic IT protection. This can be used to document that all relevant security requirements have been implemented for the information network under consideration in accordance with basic IT protection.

Source: Glossary of BSI

DE Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem ISO 27001-Zertifikate (der ISO-Standard 27001 ermöglicht eine Zertifizierung des Informationssicherheitsmanagements) und ISO 27001-Zertifikate auf der Basis von IT-Grundschutz. Damit kann dokumentiert werden, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsanforderungen gemäß IT-Grundschutz realisiert wurden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL certyfikat

Termin certyfikat jest używany w bezpieczeństwie informacji w różnych obszarach i w różnym znaczeniu. Należy odróżnić certyfikaty ISO 27001 (norma ISO 27001 umożliwia certyfikację zarządzania bezpieczeństwem informacji) od certyfikatów ISO 27001 opartych na podstawowej ochronie informatycznej. Certyfikat może być wykorzystany do udokumentowania, że wszystkie istotne wymagania bezpieczeństwa zostały wdrożone dla danej sieci informacyjnej zgodnie z podstawową ochroną informatyczną.

Źródło: Słownikf BSI

LIT sertifikatas

Sąvoka sertifikatas yra naudojama informacijos saugumui įvairiose srityse ir turi skirtingas reikšmes. Turi būti atskirti ISO 27001 sertifikatai (ISO 27001 standartas leidžia sertifikuoti informacijos saugumo valdymą) ir ISO 27001 sertifikatai, pagrįsti pagrindine IT apsauga. Tai gali būti naudojama dokumentuojant, kad pagal atitinkamą IT apsaugą nagrinėjamam informaciniam tinklui buvo įgyvendinti visi susiję saugos reikalavimai.

šaltinis: BSI žodynas

IT certificato

Il termine certificato è usato nella sicurezza dell'informazione in vari settori con diversi significati. Si deve fare una distinzione tra i certificati ISO 27001 (la norma ISO 27001 permette la certificazione della gestione della sicurezza dell'informazione) e i certificati ISO 27001 basati sulla protezione informatica di base. Quest'ultimo può essere utilizzato

per documentare che tutti i requisiti di sicurezza rilevanti sono stati implementati per la rete d'informazione in esame secondo la protezione informatica di base.

Fonte: Glossario di BSI

click fraud

Click Fraud is the generation of artificial access (clicks) to advertising banners in the Internet browser. The underlying billing systems are manipulated in this way in order to increase the revenue from the advertisements, which are paid for on the basis of access.

Source: Glossary of BSI

DE Klickbetrug

Als Klickbetrug bezeichnet man das Generieren von künstlichen Zugriffen (Klicks) auf Werbebannereinblendungen im Internetbrowser. Hierdurch werden die dahinterliegenden Abrechnungssysteme manipuliert, um die Einnahmen der nach Zugriff vergüteten Werbeeinblendungen zu steigern.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL oszustwo przez kliknięcie

Click Fraud to generowanie sztucznego dostępu (kliknięć) do banerów reklamowych w przeglądarce internetowej. W ten sposób manipuluje się podstawowymi systemami rozliczeniowymi w celu zwiększenia przychodów z reklam, które są opłacane na podstawie dostępu.

Źródło: Słownikf BSI

LIT paspaudimų sukčiavimas

Paspaudimų sukčiavimas yra dirbtinės prieigos (paspaudimų) prie reklamos reklamjuosčių generavimas interneto naršyklėje. Tokiu būdu manipuliuojama pagrindinėmis atsiskaitymo sistemomis, siekiant padidinti pajamas iš skelbimų, už kurias mokama pagal prieigą.

šaltinis: BSI žodynas

IT frode a colpi di clic

La Click Fraud è la generazione di accessi artificiali (click) ai banner pubblicitari nel browser Internet. I sistemi di fatturazione sottostanti vengono manipolati in questo modo per aumentare le entrate delle pubblicità, che vengono pagate in base agli accessi.

Fonte: Glossario di BSI

client

A client is a software or hardware that can access certain services from a server. The term client often refers to a workstation computer that accesses data and programs from servers in a network.

Source: Glossary of BSI

DE Client

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL klient

Klient to oprogramowanie lub sprzęt, który może uzyskać dostęp do pewnych usług z serwera. Termin klient często odnosi się do komputera stacji roboczej, który uzyskuje dostęp do danych i programów z serwerów w sieci.

Źródło: Słownikf BSI

LIT klientas

Klientas yra programinė įranga arba aparatinė įranga, galinti pasiekti tam tikras paslaugas iš serverio. Terminas klientas dažnai reiškia darbo vietos kompiuterį, kuris pasiekia duomenis ir programas iš tinklo serverių.

šaltinis: BSI žodynas

IT cliente

Un client è un software o un hardware che può accedere a certi servizi da un server. Il termine client si riferisce spesso a una stazione di lavoro che accede a dati e programmi dai server in una rete.

Fonte: Glossario di BSI

cloaking

The search engine manipulation algorithm. The robot is given a web page that matches the specific search terms but which is then not displayed to the searcher. As soon as the searcher clicks on the link, he is automatically redirected to another website.

Source: Glossary of BSI

DE Cloaking

Eine Methode zur Manipulation von Suchmaschinen. Dabei wird dem Robot eine Webseite als Ergebnis unterschoben, auf die die konkreten Suchbegriffe passen, die dem Suchenden dann aber nicht angezeigt wird. Sobald dieser auf den Link klickt, wird er automatisch auf eine andere Webseite umgeleitet.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL maskowanie

Algorytm manipulacji w wyszukiwarce. Robot otrzymuje stronę internetową, która odpowiada konkretnym wyszukiwanym hasłom, ale która nie jest następnie wyświetlana wyszukiwarce. Po kliknięciu na link, zostaje on automatycznie przekierowany na inną stronę.

Źródło: Słownikf BSI

LIT maskavimas

Paieškos variklio manipuliavimo algoritmas. Robotui suteikiamas tinklalapis, atitinkantis konkrečius paieškos terminus, bet kuris nerodomas ieškotojui. Kai tik ieškotojas spustelės nuorodą, jis bus automatiškai nukreiptas į kitą svetainę.

šaltinis: BSI žodynas

IT occultamento

L'algoritmo di manipolazione del motore di ricerca. Al robot viene data una pagina web che corrisponde ai termini di ricerca specifici, ma che poi non viene mostrata al ricercatore. Non appena il ricercatore clicca sul link, viene automaticamente reindirizzato a un altro sito web.

Fonte: Glossario di BSI

cloud computing

Cloud computing refers to the dynamic provision, use, and billing of IT services over a network in line with demand. These services are offered and used exclusively via defined technical interfaces and protocols. The services provided as part of cloud computing cover the entire spectrum of information technology and include infrastructures (computing power, storage space), platforms and software.

Source: Glossary of BSI

DE Cloud Computing

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL cloud computing

Cloud computing odnosi się do dynamicznego dostarczania, wykorzystywania i rozliczania usług informatycznych przez sieć zgodnie z zapotrzebowaniem. Usługi te są oferowane i wykorzystywane wyłącznie za pośrednictwem zdefiniowanych interfejsów technicznych i protokołów. Usługi świadczone w ramach cloud computingu obejmują całe spektrum technologii informacyjnych i obejmują infrastruktury (moc obliczeniową, przestrzeń dyskową), platformy i oprogramowanie.

Źródło: Słownikf BSI

LIT debesų kompiuterija

Debesų kompiuterija reiškia dinamišką IT paslaugų teikimą, naudojimą ir atsiskaitymą už tinklą, atsižvelgiant į paklausą. Šios paslaugos siūlomos ir naudojamos tik naudojant apibrėžtas technines sąsajas ir protokolus. Paslaugos, teikiamos kaip debesų kompiuterijos dalis, apima visą informacinių technologijų spektrą ir apima infrastruktūrą (skaičiavimo galią, saugojimo vietą), platformas ir programinę įrangą.

šaltinis: BSI žodynas

IT cloud computing

Il cloud computing si riferisce alla fornitura dinamica, all'uso e alla fatturazione di servizi IT su una rete in linea con la domanda. Questi servizi sono offerti e utilizzati esclusivamente attraverso interfacce tecniche e protocolli definiti. I servizi forniti come parte del cloud computing coprono l'intero spettro della tecnologia dell'informazione e comprendono infrastrutture (potenza di calcolo, spazio di archiviazione), piattaforme e software.

Fonte: Glossario di BSI

computer virus

A computer virus is a non-independent program routine that reproduces itself and thereby performs manipulations in system areas, on other programs or their environment that the user cannot control. Additionally, programmed damage functions of the virus may be present.

Source: Glossary of BSI

DE Computer-Virus

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL wirus komputerowy

Wirus komputerowy to nie niezależna procedura programowa, która powiela się i w ten sposób dokonuje manipulacji w obszarach systemu, na innych programach lub ich środowisku, których użytkownik nie może kontrolować. (Dodatkowo mogą być obecne zaprogramowane funkcje niszczące wirusa).

Źródło: Słownikf BSI

LIT kompiuterinis virusas

Kompiuterinis virusas yra nepriklausoma programų rutina, kuri dauginasi pati ir taip atlieka manipuliacijas sistemos srityse, kitose programose ar jų aplinkoje, kurių vartotojas negali kontroliuoti. (Be to, gali būti užprogramuotos viruso pažeidimo funkcijos).

šaltinis: BSI žodynas

IT virus informatico

Un virus informatico è una routine di programma non indipendente che si riproduce e quindi esegue manipolazioni in aree del sistema, su altri programmi o sul loro ambiente che l'utente non può controllare. (Inoltre, possono essere presenti funzioni di danno programmato del virus).

Fonte: Glossario di BSI

copyright

Legal regulations for the protection of creators of literary, scientific and artistic works. In particular, music, pictures, films, literature, but also representations of a scientific/technical nature (city plans, construction drawings, etc.) and software are protected. In Germany, copyright is regulated by the Copyright Act.

Source: Glossary of BSI

DE Urheberrecht

Rechtliche Regelungen zum Schutz der Schöpfer von Werken der Literatur, Wissenschaft und Kunst. Geschützt werden insbesondere Musik, Bilder, Filme, Literatur, aber auch Darstellungen wissenschaftlicher/technischer Art (Stadtpläne, Bauzeichnungen etc.) sowie Software. In Deutschland ist das Urheberrecht im Urheberrechtsgesetz geregelt.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL prawa autorskie

Regulacje prawne dotyczące ochrony twórców dzieł literackich, naukowych i artystycznych. Ochronie podlegają w szczególności muzyka, zdjęcia, filmy, literatura, ale także dzieła o charakterze naukowym/technicznym (plany miast, rysunki budowlane itp.) oraz oprogramowanie. W Niemczech prawo autorskie jest regulowane przez ustawę o prawie autorskim.

Źródło: Słownikf BSI

LIT autorių teisės

Literatūros, mokslo ir meno kūrinių kūrėjų apsaugos teisinis reglamentavimas. Ypač saugoma muzika, paveikslai, filmai, literatūra, taip pat mokslinio/techninio pobūdžio vaizdai (miesto planai, statybos brėžiniai ir kt.) Ir programinė įranga. Vokietijoje autorių teises reglamentuoja Autorių teisių įstatymas.

šaltinis: BSI žodynas

IT copyright

Norme giuridiche per la protezione dei creatori di opere letterarie, scientifiche e artistiche. In particolare, musica, immagini, film, letteratura, ma anche rappresentazioni di carattere scientifico

Fonte: Glossario di BSI

credentials

Typical examples of credentials are passwords, cryptographic keys and certificates, authentication tickets and session cookies. Credentials can be stolen, for example, due to an attack on the user database of websites or online services. Credentials can also be recorded by malware infections on clients and thus transmitted to third parties without authorization. However, devices such as smartphones, hardware tokens or mobile data carriers can also be specifically stolen if an attacker suspects credentials on these components. Authentication tickets or cookies can be intercepted via unencrypted connections.

Source: Glossary of BSI

DE Credentials

Typische Beispiele für Credentials sind Passwörter, kryptografische Schlüssel und Zertifikate, sog. "Authentisierungs-Tickets" oder auch "Session-Cookies". Ein Diebstahl von Credentials kann z.B. Folge einer Attacke auf die Benutzerdatenbank von Webseiten oder Online-Diensten sein. Credentials können auch durch Schadsoftware-Infektionen auf Clients mitgeschnitten und so unbefugt an Dritte übermittelt werden. Es können aber auch gezielt Geräte wie Smartphones, Hardware-Tokens oder mobile Datenträger gestohlen werden, wenn ein Angreifer Zugangsdaten auf diesen Komponenten vermutet. Authentisierungs-Tickets oder Cookies können über unverschlüsselte Verbindungen mitgeschnitten werden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL uwierzytelnienia

Typowymi przykładami danych uwierzytelniających są hasła, klucze kryptograficzne i certyfikaty, bilety uwierzytelniające i pliki cookie sesji. Dane uwierzytelniające mogą zostać skradzione, na przykład w wyniku ataku na bazę danych użytkowników stron internetowych lub usług online. Dane uwierzytelniające mogą być również zapisywane przez złośliwe oprogramowanie zainfekowane na klientach i w ten sposób przekazywane osobom trzecim bez upoważnienia. Urządzenia takie jak smartfony, tokeny sprzętowe lub mobilne nośniki danych mogą jednak również zostać skradzione, jeżeli atakujący podejrzewa, że dane uwierzytelniające znajdują się na tych komponentach. Bilety uwierzytelniające lub pliki cookie mogą zostać przechwycone przez nieszyfrowane połączenia.

Źródło: Słownikf BSI

LIT įgaliojimai

Įprasti kredencialų pavyzdžiai yra slaptažodžiai, kriptografiniai raktai ir sertifikatai, autentifikavimo bilietai ir sesijos slapukai. Įgaliojimai gali būti pavogti, pavyzdžiui, dėl atakos prieš svetainių ar internetinių paslaugų vartotojų duomenų bazę. Kliento duomenis taip pat galima įrašyti į klientų kenkėjiškas programas ir taip be leidimo perduoti trečiosioms šalims. Tačiau tokius įrenginius kaip išmanieji telefonai, techninės įrangos žetonai ar mobiliosios duomenų laikmenos taip pat galima specialiai pavogti, jei užpuolikas įtaria šių komponentų įgaliojimus. Autentifikavimo bilietai ar slapukai gali būti perimami naudojant nešifruotus ryšius.

IT credenziali

Esempi tipici di credenziali sono password, chiavi crittografiche e certificati, ticket di autenticazione e cookie di sessione. Le credenziali possono essere rubate, per esempio, a causa di un attacco al database degli utenti di siti web o servizi online. Le credenziali possono anche essere registrate da infezioni malware sui client e quindi trasmesse a terzi senza autorizzazione. Tuttavia, anche i dispositivi come gli smartphone, i token hardware o i supporti dati mobili possono essere specificamente rubati se un aggressore sospetta le credenziali su questi componenti. I ticket di autenticazione o i cookie possono essere intercettati attraverso connessioni non cifrate.

Fonte: Glossario di BSI

cryptography

Science of encrypting information in "secret scripts". The purpose is to prevent third parties from viewing information that is not intended for them. Various encryption systems are used on the Internet to ensure secure data exchange and protect confidential information. Cryptographic processes are also used for digital signatures.

Source: Glossary of BSI

DE Kryptographie

Wissenschaft der Verschlüsselung von Informationen in "Geheimschriften". Damit soll verhindert werden, dass Dritte Informationen einsehen können, die nicht für sie bestimmt sind. Im Internet werden verschiedene Verschlüsselungssysteme eingesetzt, um einen sicheren Datenaustausch zu gewährleisten und vertrauliche Informationen zu schützen. Kryptographische Verfahren kommen auch bei der digitalen Signatur zum Einsatz.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL kryptografia

Nauka o szyfrowaniu informacji w "tajnych skryptach". Ma to na celu uniemożliwienie osobom trzecim wglądu w informacje, które nie są dla nich przeznaczone. W Internecie stosowane są różne systemy szyfrowania w celu zapewnienia bezpiecznej wymiany danych i ochrony poufnych informacji. Procesy kryptograficzne są również wykorzystywane do podpisów cyfrowych.

Źródło: Słownikf BSI

LIT kriptografija

Informacijos šifravimo „slaptuose scenarijuose" mokslas. Tikslas - neleisti trečiosioms šalims peržiūrėti jiems neskirtos informacijos. Siekiant užtikrinti saugų keitimąsi duomenimis ir apsaugoti konfidencialią informaciją, internete naudojamos įvairios šifravimo sistemos. Kriptografiniai procesai taip pat naudojami skaitmeniniams parašams.

šaltinis: BSI žodynas

IT crittografia

Scienza della crittografia delle informazioni in "script segreti". Lo scopo è quello di impedire a terzi di visualizzare informazioni che non sono destinate a loro. Diversi sistemi di crittografia sono utilizzati su Internet per garantire uno scambio di dati sicuro e proteggere le informazioni riservate. I processi crittografici sono utilizzati anche per le firme digitali.

Fonte: Glossario di BSI

cyber security

Cybersecurity deals with all aspects of security in information and communications technology. The field of action of information security is thereby extended to the entire cyberspace. This encompasses all information technology connected to the Internet and comparable networks and includes communications, applications, processes and processed information based on them. When considering cybersecurity, a special focus is often placed on attacks from cyberspace.

Source: Glossary of BSI

DE Cyber-Sicherheit

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne dotyczy wszystkich aspektów bezpieczeństwa w technologiach informacyjnych i komunikacyjnych. Obszar działania bezpieczeństwa informacji rozszerza się tym samym na całą cyberprzestrzeń. Obejmuje to wszystkie technologie informatyczne podłączone do Internetu i porównywalnych sieci, w tym komunikację, aplikacje, procesy i przetwarzane na ich podstawie informacje. Przy rozważaniach dotyczących bezpieczeństwa cybernetycznego szczególny nacisk kładzie się często na ataki z cyberprzestrzeni.

Źródło: Słownikf BSI

LIT Kibernetinė sauga

Kibernetinis saugumas susijęs su visais informacijos ir ryšių technologijų saugumo aspektais. Informacijos saugumo veiksmų sritis yra išplėsta į visą elektroninę erdvę. Tai apima visas prie interneto ir panašių tinklų prijungtas informacines technologijas, įskaitant ryšius, programas, procesus ir jais pagrįstą apdorotą informaciją. Svarstant kibernetinį saugumą, ypatingas dėmesys dažnai skiriamas kibernetinės erdvės atakoms.

šaltinis: BSI žodynas

IT sicurezza informatica

La cybersecurity si occupa di tutti gli aspetti della sicurezza nella tecnologia dell'informazione e della comunicazione. Il campo d'azione della sicurezza dell'informazione è quindi esteso all'intero cyberspazio. Questo comprende tutte le tecnologie dell'informazione collegate a Internet e a reti analoghe e comprende le comunicazioni, le applicazioni, i processi e le informazioni elaborate basate su di esse. Quando si considera la cybersecurity, un'attenzione particolare è spesso rivolta agli attacchi dal cyberspazio.

Fonte: Glossario di BSI

data leak

When data is leaked, it falls into the wrong hands. Cybercriminals can get hold of this data via a compromised website or via a breakdown in which a company keeps sensitive data unprotected. In some cases, the sensitive data is then also published.

Source: Glossary of BSI

DE Datenleak

Bei einem Datenleak geraten Daten in falsche Hände. Cyberkriminelle können über eine kompromittierte Webseite an diese Daten kommen oder über eine Panne, bei der ein Unternehmen die sensiblen Daten ungeschützt aufbewahrt. Teilweise werden die sensiblen Daten dann auch veröffentlicht.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL wyciek danych

Kiedy dane wyciekają, dostają się w niepowołane ręce. Cyberprzestępcy mogą wejść w posiadanie tych danych za pośrednictwem zagrożonej strony internetowej lub awarii, w której firma przechowuje wrażliwe dane bez ochrony. W niektórych przypadkach dane wrażliwe są następnie publikowane.

Źródło: Słownikf BSI

LIT duomenų nutekėjimas

Nutekėję duomenys patenka į netinkamas rankas. Kibernetiniai nusikaltėliai gali gauti šiuos duomenis per pažeistą svetainę arba per suskirstymą, kuriame įmonė saugo neskelbtinus duomenis. Kai kuriais atvejais neskelbtini duomenys taip pat skelbiami.

šaltinis: BSI žodynas

IT fuga di dati

Quando i dati trapelano, cadono nelle mani sbagliate. I criminali informatici possono entrare in possesso di questi dati attraverso un sito web compromesso o attraverso un guasto in cui un'azienda mantiene dati sensibili non protetti. In alcuni casi, i dati sensibili vengono poi anche pubblicati.

Fonte: Glossario di BSI

data miner

Program for collecting, filtering and transmitting specific data from internal company databases and external information sources. The data miner then searches for patterns and correlations in the data obtained, thereby gaining new information. The clients are companies that use the data to analyze and predict behaviors and trends and to support decision-making.

Source: Glossary of BSI

DE Data Miner

Programm zum Sammeln, Herausfiltern und Übermitteln von bestimmten Daten aus internen Unternehmensdatenbanken und externen Informationsquellen. In den gewonnenen Daten sucht der Data Miner anschließend nach Mustern und Zusammenhängen und gewinnt dadurch neue Informationen. Auftraggeber sind Unternehmen, die die Daten zur Analyse und Vorhersage von Verhaltensweisen und Trends und als Entscheidungshilfe nutzen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL miner danych

Program do zbierania, filtrowania i przesyłania określonych danych z wewnętrznych baz danych firmy oraz zewnętrznych źródeł informacji. Następnie data miner poszukuje wzorców i korelacji w uzyskanych danych, uzyskując w ten sposób nowe informacje. Klientami są firmy, które wykorzystują dane do analizowania i przewidywania zachowań i trendów oraz wspomagania podejmowania decyzji.

Źródło: Słownikf BSI

LIT duomenų kasėjas

Programa, skirta rinkti, filtruoti ir perduoti konkrečius duomenis iš vidinių įmonės duomenų bazių ir išorinių informacijos šaltinių. Tada duomenų kasėjas ieško gautų duomenų modelių ir koreliacijų, taip įgydamas naujos informacijos. Klientai yra įmonės, kurios naudoja duomenis analizuoti ir prognozuoti elgesį ir tendencijas bei remti sprendimų priėmimą.

šaltinis: BSI žodynas

IT minatore di dati

Programma per la raccolta, il filtraggio e la trasmissione di dati specifici da banche dati aziendali interne e fonti di informazione esterne. Il data miner cerca poi modelli e correlazioni nei dati ottenuti, ottenendo così nuove informazioni. I clienti sono aziende che utilizzano i dati per analizzare e prevedere comportamenti e tendenze e per sostenere il processo decisionale.

Fonte: Glossario di BSI

data owner

A data manager is responsible for a specific data collection of the office (e.g. data of the social sector). Often this role is assigned to the application manager.

Source: dsb – Zurich

DE Datenverantwortliche/r

Ein/e Datenverantwortliche/r ist für eine bestimmte Datensammlung der Amtsstelle verantwortlich (z.B. Daten des Sozialbereichs). Oft wird diese Rolle der/dem Anwendungsverantwortlichen zugewiesen.

Quelle: dsb - Datenschutzbeauftragte Kanton Zürich

POL właściciel danych

Administrator danych jest odpowiedzialny za konkretny zbiór danych urzędu (np. dane sektora socjalnego). Często rola ta jest przypisana do kierownika ds. realizacji.

Źródło: dsb - Zürich

LIT duomenų savininkas

Duomenų valdytojas yra atsakingas už tam tikrą biuro duomenų rinkimą (pvz., socialinio sektoriaus duomenis). Dažnai šis vaidmuo priskiriamas programų valdytojui.

šaltinis: dsb - Zürich

IT proprietario dei dati

Un data manager è responsabile di una specifica raccolta di dati dell'ufficio (per esempio i dati del settore sociale). Spesso questo ruolo è assegnato al responsabile delle applicazioni.

Fonte: dsb - Zurigo

data protection management system

A DSMS is a set of procedures and rules within an office that serve to ensure data protection and information security on a permanent basis.

Source: dsb - Zurich

DE Datenschutz-Managementsystem (DSMS)

Ein DSMS ist eine Aufstellung von Verfahren und Regeln innerhalb einer Amtsstelle, die dazu dienen, den Datenschutz und die Informationssicherheit dauerhaft zu gewährleisten.

Quelle: dsb - Zürich

POL system zarządzania ochroną danych

DSMS to zbiór procedur i zasad obowiązujących w biurze, które służą stałemu zapewnieniu ochrony danych i bezpieczeństwa informacji.

Źródło: dsb - Zürich

LIT duomenų apsaugos valdymo sistema

DSMS yra biure esančių procedūrų ir taisyklių rinkinys, skirtas nuolat užtikrinti duomenų apsaugą ir informacijos saugumą.

šaltinis: dsb - Zürich

IT sistema di gestione della protezione dei dati

Un DSMS è un insieme di procedure e regole all'interno di un ufficio che servono a garantire la protezione dei dati e la sicurezza delle informazioni su base permanente.

Fonte: dsb - Zurigo

data protection officer

Data protection officers are internal specialists, also known as data protection advisors, who deal with data protection issues.

Source: dsb - Zurich

DE Datenschutzverantwortlicher (DSV)

Bei den Datenschutzverantwortlichen handelt es sich um interne Spezialistinnen und Spezialisten, auch Datenschutzberater/innen genannt, die sich um Datenschutzfragen kümmern.

Quelle: dsb - Zürich

POL inspektor ochrony danych

Inspektorzy ochrony danych to wewnętrzni specjaliści, znani również jako doradcy ds. ochrony danych, którzy zajmują się kwestiami ochrony danych.

Źródło: dsb - Zürich

LIT duomenų apsaugos pareigūnas

Duomenų apsaugos pareigūnai yra vidaus specialistai, dar vadinami duomenų apsaugos patarėjais, kurie sprendžia duomenų apsaugos klausimus.

šaltinis: dsb - Zürich

IT responsabile della protezione dei dati

I responsabili della protezione dei dati sono specialisti interni, noti anche come consulenti per la protezione dei dati, che si occupano di questioni relative alla protezione dei dati.

Fonte: dsb - Zurigo

data protection

Data protection is intended to protect individuals from having their personal rights infringed by the handling of their personal data. Data protection therefore refers to the protection of personal data against possible misuse by third parties (not to be confused with data security).

Source: Glossary of BSI

DE Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Quelle: Glossar der Cyber-Sicherheit – BSI

POL ochrona danych

Ochrona danych ma na celu ochronę osób fizycznych przed naruszeniem ich praw osobistych w związku z przetwarzaniem ich danych osobowych. Ochrona danych odnosi się zatem do ochrony danych osobowych przed możliwym niewłaściwym wykorzystaniem przez strony trzecie (nie należy jej mylić z bezpieczeństwem danych).

Źródło: Słownikf BSI

LIT duomenų apsauga

Duomenų apsauga skirta apsaugoti asmenis nuo jų asmeninių teisių pažeidimo tvarkant jų asmens duomenis. Todėl duomenų apsauga reiškia asmens duomenų apsaugą nuo galimo trečiųjų šalių piktnaudžiavimo (nepainiokite su duomenų saugumu).

šaltinis: BSI žodynas

IT protezione dei dati

La protezione dei dati ha lo scopo di proteggere le persone dalla violazione dei loro diritti personali attraverso il trattamento dei loro dati personali. La protezione dei dati si riferisce quindi alla protezione dei dati personali contro possibili abusi da parte di terzi (da non confondere con la sicurezza dei dati).

Fonte: Glossario di BSI

data security

Protection of data with regard to given requirements for their confidentiality, availability and integrity (other term: information security).

Source: Glossary of BSI

DE Datensicherheit

Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität (anderer Begriff: Informationssicherheit).

Quelle: Glossar der Cyber-Sicherheit – BSI

POL bezpieczeństwo danych

Ochrona danych z uwzględnieniem określonych wymagań dotyczących ich poufności, dostępności i integralności (inny termin: bezpieczeństwo informacji).

Źródło: Słownikf BSI

LIT duomenų saugumas

Duomenų saugumas atsižvelgiant į jų konfidencialumo, prieinamumo ir vientisumo reikalavimus (kitas terminas: informacijos saugumas).

šaltinis: BSI žodynas

IT sicurezza dei dati

Protezione dei dati in relazione a determinati requisiti per la loro riservatezza, disponibilità e integrità (altro termine: sicurezza delle informazioni).

Fonte: Glossario di BSI

decryption

Process in which electronic data is made readable or processable again using mathematical algorithms and private or secret keys. In encrypted form, the data cannot be viewed by unauthorized third parties. The data can only be restored to its original form by the owner of the corresponding private or secret key.

Source: Glossary of BSI

DE Entschlüsselung

Vorgang, bei dem unter Verwendung mathematischer Algorithmen und privater oder geheimer Schlüssel elektronische Daten wieder les- bzw. verarbeitbar gemacht werden. In verschlüsselter Form sind die Daten von unbefugten Dritten nicht einsehbar. Die Daten können nur vom Besitzer des entsprechenden privaten oder geheimen Schlüssels wieder in die Originalform überführt werden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL rozszyfrowanie

Proces, w którym dane elektroniczne stają się ponownie czytelne lub możliwe do przetworzenia przy użyciu algorytmów matematycznych i kluczy prywatnych lub tajnych. W formie zaszyfrowanej dane nie mogą być przeglądane przez nieuprawnione osoby trzecie. Dane mogą zostać przywrócone do ich pierwotnej postaci tylko przez właściciela odpowiedniego klucza prywatnego lub tajnego.

Źródło: Słownikf BSI

LIT iššifravimas

Procesas, kurio metu elektroniniai duomenys daromi skaitomi arba vėl apdorojami naudojant matematinius algoritmus ir asmeninius arba slaptus raktus. Užšifruota forma duomenų negali peržiūrėti neleistinos trečiosios šalys. Duomenis pradine forma gali atkurti tik atitinkamo privataus ar slapto rakto savininkas.

šaltinis: BSI žodynas

IT decrittazione

Processo in cui i dati elettronici sono resi nuovamente leggibili o processabili usando algoritmi matematici e chiavi private o segrete. In forma criptata, i dati non possono essere visti da terzi non autorizzati. I dati possono essere ripristinati nella loro forma originale solo dal proprietario della chiave privata o segreta corrispondente.

Fonte: Glossario di BSI

encryption

Encryption transforms a plaintext depending on an additional information called "key" into an associated ciphertext, which should be indecipherable to those who do not know the key. The reverse transformation - the recovery of the plaintext from the ciphertext - is called decryption.

Source: Glossary of BSI

DE Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL szyfrowanie

Szyfrowanie przekształca tekst jawny w zależności od dodatkowej informacji zwanej "kluczem" w powiązany z nim szyfrogram, który powinien być nie do rozszyfrowania dla osób nie znających klucza. Odwrotna transformacja - odzyskanie tekstu jawnego z szyfrogramu - nazywana jest rozszyfrowaniem.

Źródło: Słownikf BSI

LIT šifravimas

Šifravimas paverčia paprastą tekstą, priklausomai nuo papildomos informacijos, vadinamos „raktu“, į susijusį šifruotą tekstą, kuris turėtų būti neiššifruojamas tiems, kurie to rakto nežino. Atvirkštinė transformacija - paprasto teksto atkūrimas iš šifruoto teksto - vadinamas iššifravimu.

šaltinis: BSI žodynas

IT crittografia

La crittografia trasforma un testo in chiaro in funzione di un'informazione supplementare chiamata "chiave" in un testo cifrato associato, che dovrebbe essere indecifrabile per chi non conosce la chiave. La trasformazione inversa - il recupero del testo in chiaro dal testo cifrato - si chiama decrittazione.

Fonte: Glossario di BSI

end-to-end encryption

End-to-end encryption is end-to-end encryption between sender and recipient. The term is encountered primarily in e-mail communication. In order to use end-to-end encryption, the sender and recipient need appropriate encryption software and must have the respective public key of the communication partner. The best-known methods are S/MIME and PGP.

Source: Glossary of BSI

DE Ende-zu-Ende-Verschlüsselung

Die Ende-zu-Ende-Verschlüsselung ist eine durchgängige Verschlüsselung zwischen Absender und Empfänger. Den Begriff trifft man vor allem bei der E-Mail-Kommunikation an. Um Ende-zu-Ende-Verschlüsselung verwenden zu können, benötigen Absender und Empfänger entsprechende Verschlüsselungssoftware und müssen den jeweils öffentlichen Schlüssel des Kommunikationspartners besitzen. Die bekanntesten Verfahren sind S/MIME und PGP.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL szyfrowanie typu "end-to-end"

End-to-end encryption to szyfrowanie na całej drodze pomiędzy nadawcą a odbiorcą. Termin ten spotykany jest przede wszystkim w komunikacji e-mailowej. Aby móc korzystać z szyfrowania end-to-end, nadawca i odbiorca potrzebują odpowiedniego oprogramowania szyfrującego i muszą posiadać odpowiedni klucz publiczny partnera komunikacji. Najbardziej znanymi metodami są S/MIME i PGP.

Źródło: Słownikf BSI

LIT ištisinis šifravimas

Ištisinis šifravimas vykdomas tarp siuntėjo ir gavėjo. Šis terminas pirmiausia sutinkamas bendraujant el. pašto priemonėmis. Norint naudoti ištisinį šifravimą siuntėjui ir gavėjui reikia tinkamos šifravimo programinės įrangos. Taip pat jie turi turėti atitinkamą viršąjį raktą. Žinomiausi metodai yra S/MIME ir PGP.

šaltinis: BSI žodynas

IT crittografia end-to-end

La crittografia end-to-end è la crittografia end-to-end tra mittente e destinatario. Il termine si incontra principalmente nella comunicazione via e-mail. Per utilizzare la crittografia end-to-end, il mittente e il destinatario hanno bisogno di un software di crittografia appropriato e devono avere la rispettiva chiave pubblica del partner di comunicazione.

Fonte: Glossario di BSI

exploit

An exploit is a method or program code that can be used to execute unintended commands or functions via a vulnerability in hardware or software components. Depending on the type of vulnerability, an exploit can be used, for example, to crash a program, extend user privileges, or execute arbitrary program code.

Source: Glossary of BSI

DE Exploit

Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL exploit

Exploit to metoda lub kod programu, który może zostać wykorzystany do wykonania niezamierzonych poleceń lub funkcji za pośrednictwem luki w komponentach sprzętowych lub programowych. W zależności od typu luki, exploit może zostać wykorzystany na przykład do uszkodzenia programu, rozszerzenia uprawnień użytkownika lub wykonania dowolnego kodu programu.

Źródło: Słownikf BSI

LIT išnaudoti

Išnaudojimas yra metodas arba programos kodas, kuris gali būti naudojamas netyčinėms komandoms ar funkcijoms vykdyti per aparatūros ar programinės įrangos komponentų pažeidžiamumą. Priklausomai nuo pažeidžiamumo tipo, išnaudojimas gali būti naudojamas, pavyzdžiui, norint sugadinti programą, išplėsti vartotojo teises ar įvykdyti savavališką programos kodą.

šaltinis: BSI žodynas

IT sfruttare

Un exploit è un metodo o un codice di programma che può essere usato per eseguire comandi o funzioni non volute attraverso una vulnerabilità in componenti hardware o software. A seconda del tipo di vulnerabilità, un exploit può essere usato, per esempio, per bloccare un programma, estendere i privilegi dell'utente o eseguire codice arbitrario del programma.

Fonte: Glossario di BSI

Federal Office for Information Security

Founded in 1999, the Federal Office is part of the Federal Ministry of the Interior and is an independent and neutral body for issues relating to IT security in the information society. The BSI investigates security risks in the use of information technology and develops security measures.

Source: Glossary of BSI

DE Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das 1999 gegründete Bundesamt gehört zum Geschäftsbereich des Bundesministerium des Innern und ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL Federalny Urząd ds. Bezpieczeństwa Informacji

Założony w 1999 roku Urząd Federalny jest częścią Federalnego Ministerstwa Spraw Wewnętrznych i jest niezależnym i neutralnym organem zajmującym się kwestiami związanymi z bezpieczeństwem IT w społeczeństwie informacyjnym. BSI bada zagrożenia bezpieczeństwa przy korzystaniu z technologii informatycznych i opracowuje środki bezpieczeństwa.

Źródło: Słownikf BSI

LIT Federalinis informacijos saugumo biuras

Federalinis biuras, įkurtas 1999 m., Yra Federalinės vidaus reikalų ministerijos dalis ir yra nepriklausoma ir neutrali institucija sprendžiant su IT saugumu informacinėje visuomenėje susijusius klausimus. BSI tiria saugumo riziką naudojant informacines technologijas ir kuria saugumo priemones.

šaltinis: BSI žodynas

IT Ufficio federale per la sicurezza delle informazioni

Fondato nel 1999, l'Ufficio federale fa parte del Ministero federale dell'interno ed è un organo indipendente e neutrale per le questioni relative alla sicurezza informatica nella società dell'informazione. Il BSI indaga sui rischi di sicurezza nell'uso delle tecnologie dell'informazione e sviluppa misure di sicurezza.

Fonte: Glossario di BSI

file

Related data created, for example, with an application program and stored under a file name on the disk. All data on a disk is organized in the form of files (and directories).

Source: Glossary of BSI

DE Datei

Zusammengehörende Daten, die beispielsweise mit einem Anwendungsprogramm erstellt und unter einem Datei-Namen auf dem Datenträger gespeichert werden. Alle Daten auf einem Datenträger sind in Form von Dateien (und Verzeichnissen) organisiert.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL plik

Powiązane dane tworzone np. za pomocą programu użytkowego i przechowywane na dysku pod nazwą pliku. Wszystkie dane na dysku są zorganizowane w postaci plików (i katalogów).

Źródło: Słownikf BSI

LIT failas

Susiję duomenys, sukurti, pavyzdžiui, naudojant taikomąją programą, ir saugomi diske failo pavadinimu. Visi diske esantys duomenys yra suskirstyti į failus (ir katalogus).

šaltinis: BSI žodynas

IT file

Dati correlati creati, per esempio, con un programma applicativo e memorizzati con un nome di file sul disco. Tutti i dati su un disco sono organizzati sotto forma di file (e directory).

Fonte: Glossario di BSI

file transfer protocol

Protocol for transferring files to and from remote computers.

Source: Glossary of BSI

DE Datenübertragungsprotokoll

Protokoll zur Dateiübertragung von und zu entfernten Rechnern.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL protokół przesyłania plików

Protokół służący do przesyłania plików do i z komputerów zdalnych.

Źródło: Słowniczek BSI

LIT failas

Susiję duomenys, sukurti, pavyzdžiui, naudojant taikomąją programą, ir saugomi diske failo pavadinimu. Visi diske esantys duomenys yra suskirstyti į failus (ir katalogus).

šaltinis: BSI žodynas

IT protocollo di trasferimento file

Protocollo per il trasferimento di file da e verso computer remoti.

Fonte: Glossario di BSI

firewall

A firewall (often referred to as a security gateway) is a system of software and hardware components to securely couple IP networks (see Security gateway). The firewall consists of hardware and software that controls the flow of data between the internal network and the external network. All data leaving the network can be checked, as well as those that want to enter.

Source: Glossary of BSI

DE Firewall

Eine Firewall (oft auch als Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (siehe Sicherheitsgateway). Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden, wie die, die hineinwollen.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL firewall

Firewall (często określany jako brama bezpieczeństwa) to system składający się z oprogramowania i komponentów sprzętowych służący do bezpiecznego łączenia sieci IP (patrz Brama bezpieczeństwa). Firewall składa się ze sprzętu i oprogramowania, które kontroluje przepływ danych pomiędzy siecią wewnętrzną a siecią zewnętrzną. Wszystkie dane opuszczające sieć mogą być sprawdzane, jak również te, które chcą do niej wejść.

Źródło: Słownikf BSI

LIT ugniasienė

Ugniasienė (dažnai vadinama saugumo šliuzu) yra programinės ir techninės įrangos komponentų sistema, skirta saugiai susieti IP tinklus (žr. Apsaugos šliuzas). Ugniasienę sudaro aparatinė ir programinė įranga, kuri valdo duomenų srautą tarp vidinio tinklo ir išorinio tinklo. Jos pagalba galima patikrinti įeinančių ir išeinančių duomenų srautus tinkle.

šaltinis: BSI žodynas

IT firewall

Un firewall (spesso indicato come security gateway) è un sistema di componenti software e hardware per accoppiare in modo sicuro le reti IP (vedi Security gateway). Il firewall consiste di hardware e software che controllano il flusso di dati tra la rete interna e la rete esterna. Tutti i dati che lasciano la rete possono essere controllati, così come quelli che vogliono entrare.

Fonte: Glossario di BSI

firmware

Software that is embedded in electronic devices. Depending on the device, firmware can contain the functional scope of e.g. BIOS, operating system or application software. Firmware is specifically tailored to the respective hardware and cannot be replaced at will.

Source: Glossary of BSI

DE Firmware

Software, die in elektronische Geräte eingebettet ist. Je nach Gerät kann Firmware den Funktionsumfang von z.B. BIOS, Betriebssystem oder Anwendungssoftware enthalten. Firmware ist speziell auf die jeweilige Hardware zugeschnitten und nicht beliebig austauschbar.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL oprogramowanie układowe

Oprogramowanie, które jest wbudowane w urządzenia elektroniczne. W zależności od urządzenia, firmware może zawierać zakres funkcjonalny np. BIOS, system operacyjny lub oprogramowanie aplikacyjne. Oprogramowanie firmware jest specjalnie dostosowane do danego sprzętu i nie może być dowolnie wymieniane.

Źródło: Słownikf BSI

LIT gamyklinė įranga

Gamintojo sukurta programinė įranga, įterpta į elektroninius prietaisus. Priklausomai nuo įrenginio, programinėje įrangoje gali būti funkcinė sritis, pvz. BIOS, operacinė sistema arba taikomoji programinė įranga. Gamyklinė įranga yra specialiai pritaikyta atitinkamai aparatinei įrangai ir negali būti pakeista savo nuožiūra.

šaltinis: BSI žodynas

IT firmware

Software che è incorporato nei dispositivi elettronici. A seconda del dispositivo, il firmware può contenere l'ambito funzionale ad esempio del BIOS, del sistema operativo o del software applicativo. Il firmware è specificamente adattato al rispettivo hardware e non può essere sostituito a piacere.

Fonte: Glossario di BSI

Hardware Security Module

An HSM is a specialized piece of hardware that allows cryptographic keys to be stored in a particularly secure form and applied in a performant manner.

Source: Glossary of BSI

DE Hardware Sicherheitsmodul (HSM)

Ein HSM ist eine spezialisierte Hardware, die es ermöglicht, kryptographische Schlüssel in besonders sicherer Form aufzubewahren und performant anzuwenden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL Moduł bezpieczeństwa sprzętowego

HSM jest wyspecjalizowanym elementem sprzętowym, który umożliwia przechowywanie kluczy kryptograficznych w szczególnie bezpiecznej formie i stosowanie ich w sposób wydajny.

Źródło: Słownikf BSI

LIT techninės įrangos apsaugos modulis

HSM yra specializuota aparatinė įranga, leidžianti saugoti kriptografinius raktus ypač saugioje formoje ir efektyviai juos pritaikyti.

šaltinis: BSI žodynas

IT Modulo di sicurezza hardware

Un HSM è un pezzo di hardware specializzato che permette alle chiavi crittografiche di essere memorizzate in una forma particolarmente sicura e applicate in modo performante.

Fonte: Glossario di BSI

hoax

The term hoax refers to a false report (rumor or hoax) that is spread via e-mail, messenger programs, SMS or MMS.

Source: Glossary of BSI

DE Hoax

Der Begriff Hoax bezeichnet eine Falschmeldung (Gerücht oder Scherz), die über E-Mail, Messenger-Programme, SMS oder MMS verbreitet wird.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL hoax

Termin hoax odnosi się do fałszywego raportu (plotki lub hoax), który jest rozprzestrzeniany za pośrednictwem poczty elektronicznej, komunikatorów, SMS lub MMS.

Źródło: Słownikf BSI

LIT apgaulė

Sąvoka apgaulė reiškia klaidingą pranešimą (gandą ar apgaulę), kuris platinamas el. paštu, „Messenger" programomis, SMS ar MMS.

šaltinis: BSI žodynas

IT hoax

Il termine bufala si riferisce a una notizia falsa (diceria o bufala) che viene diffusa via e-mail, programmi di messaggeria, SMS o MMS.

Fonte: Glossario di BSI

hybrid encryption

Encryption method that uses public-key cryptography to transport keys for a symmetric encryption method, which in turn is used to encrypt the message.

Source: Glossary of BSI

DE Hybride Verschlüsselung

Verschlüsselungsverfahren, das Public-Key-Kryptographie zum Schlüsseltransport für ein symmetrisches Verschlüsselungsverfahren nutzt, welches wiederum zur Verschlüsselung der Nachricht verwendet wird.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL szyfrowanie hybrydowe

Metoda szyfrowania, która wykorzystuje kryptografię klucza publicznego do transportu kluczy dla symetrycznej metody szyfrowania, która z kolei jest używana do szyfrowania wiadomości.

Źródło: Słownikf BSI

LIT hibridinis šifravimas

Šifravimo metodas, kuris naudoja viešojo rakto kriptografiją, kad gautų raktus simetriniam šifravimo metodui, kuris savo ruožtu naudojamas šifruoti pranešimą.

šaltinis: BSI žodynas

IT crittografia ibrida

Metodo di crittografia che utilizza la crittografia a chiave pubblica per trasportare le chiavi per un metodo di crittografia simmetrica, che a sua volta viene utilizzato per crittografare il messaggio.

Fonte: Glossario di BSI

Information Security Guideline

The guideline is a central document for the information security of an institution. It describes for what purposes, by what means and with what structures information security is to be established within the institution. It contains the information security goals aimed at by the institution as well as the security strategy pursued. The security guideline thus also describes the desired level of security in an authority or company via the security objectives.

Source: Glossary of BSI

DE Leitlinie zur Informationssicherheit

Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL Wytyczne dotyczące bezpieczeństwa informacji

Wytyczne są centralnym dokumentem dotyczącym bezpieczeństwa informacji w danej instytucji. Opisują, do jakich celów, za pomocą jakich środków i przy użyciu jakich struktur ma zostać ustanowione bezpieczeństwo informacji w instytucji. Dokument zawiera cele dotyczące bezpieczeństwa informacji, do których dąży instytucja, jak również realizowaną strategię bezpieczeństwa. W ten sposób wytyczne dotyczące bezpieczeństwa opisują również pożądany poziom bezpieczeństwa w instytucji lub przedsiębiorstwie poprzez cele bezpieczeństwa.

Źródło: Słownikf BSI

LIT Informacijos saugumo gairės

Gairės yra pagrindinis institucijos informacijos saugumo dokumentas. Jame aprašoma, kokiais tikslais, kokiomis priemonėmis ir kokiomis struktūromis įstaigoje turi būti įtvirtintas informacijos saugumas. Jame pateikiami institucijos siekiami informacijos saugumo tikslai ir siekiama saugumo strategija. Taigi saugumo gairėse taip pat aprašomas pageidaujamas institucijos ar įmonės saugumo lygis siekiant saugumo tikslų.

šaltinis: BSI žodynas

IT Linea guida sulla sicurezza delle informazioni

La linea guida è un documento centrale per la sicurezza delle informazioni di un'istituzione. Descrive per quali scopi, con quali mezzi e con quali strutture la sicurezza dell'informazione deve essere stabilita all'interno dell'istituzione. Contiene gli obiettivi di sicurezza dell'informazione a cui mira l'istituzione e la strategia di sicurezza perseguita. La direttiva di sicurezza descrive quindi anche il livello di sicurezza desiderato in un'autorità o in un'azienda attraverso gli obiettivi di sicurezza.

Fonte: Glossario di BSI

integrity

The confirmation that data which has been sent, received, or stored are complete and unchanged.

Source: Glossary of BSI

DE Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL integralność

Potwierdzenie, że dane, które zostały wysłane, otrzymane lub przechowywane są kompletne i niezmienione.

Źródło: Słownikf BSI

LIT vientisumas

Patvirtinimas, kad išsiųsti, gauti ar saugomi duomenys yra išsamūs ir nepakitę.

šaltinis: BSI žodynas

IT integrità

La conferma che i dati che sono stati inviati, ricevuti o immagazzinati sono completi e invariati.

Fonte: Glossario di BSI

IT Security Officer

An IT Security Officer is responsible for aspects related to IT security in large institutions, in close coordination with IT operations. The ISB designs information security management and draws up the general security goals and specifications, while an IT security officer ensures that these are implemented technically. An IT security officer is thus typically active in IT operations, while the ISB works directly with the management level.

Source: Glossary of BSI

DE Beauftragter für IT-Sicherheit

Person mit Fachkompetenz zur IT-Sicherheit, die in großen Institutionen für Aspekte rund um die IT-Sicherheit zuständig ist, in enger Abstimmung mit dem IT-Betrieb. Der ISB gestaltet das Informationssicherheitsmanagement und erstellt die generellen Sicherheitsziele und -vorgaben, ein Beauftragter für die IT-Sicherheit sorgt dafür, dass diese technisch umgesetzt werden. Ein Beauftragter für die IT-Sicherheit ist somit typischerweise im IT-Betrieb tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL Specjalista ds. bezpieczeństwa IT

Specjalista ds. bezpieczeństwa IT jest odpowiedzialny za aspekty związane z bezpieczeństwem IT w dużych instytucjach, w ścisłej koordynacji z operacjami informatycznymi. ISB projektuje zarządzanie bezpieczeństwem informacji i opracowuje ogólne cele i specyfikacje bezpieczeństwa, podczas gdy specjalista ds. bezpieczeństwa IT zapewnia ich techniczną realizację. Specjalista ds. bezpieczeństwa IT jest zatem zazwyczaj aktywny w operacjach IT, podczas gdy ISB współpracuje bezpośrednio z kierownictwem.

Źródło: Słownikf BSI

LIT IT saugumo pareigūnas

IT saugumo pareigūnas yra atsakingas už aspektus, susijusius su IT saugumu didelėse institucijose, glaudžiai derindamas su IT operacijomis. ISB projektuoja informacijos saugumo valdymą ir nustato bendrus saugumo tikslus bei specifikacijas, o IT saugumo pareigūnas užtikrina, kad jie būtų įgyvendinami techniškai. Taigi IT saugumo pareigūnas paprastai atlieka IT operacijas, o ISB tiesiogiai dirba su valdymo lygiu.

šaltinis: BSI žodynas

IT

Un responsabile della sicurezza informatica è responsabile degli aspetti relativi alla sicurezza informatica nelle grandi istituzioni, in stretto coordinamento con le operazioni informatiche. L'ISB progetta la gestione della sicurezza delle informazioni ed elabora gli obiettivi e le specifiche generali di sicurezza, mentre un responsabile della sicurezza informatica assicura che questi siano implementati tecnicamente. Un responsabile della sicurezza informatica è quindi tipicamente attivo nelle operazioni informatiche, mentre l'ISB lavora direttamente con il livello dirigenziale.

Fonte: Glossario di BSI

keylogger

Hardware or software for recording keystrokes. All keystrokes are recorded so that they can be transmitted to an attacker as unnoticed as possible. The attacker can then use this information to filter out data that is important to him, such as login information or credit card numbers.

Source: Glossary of BSI

DE Keylogger

Hard- oder Software zum Mitschneiden von Tastatureingaben. Es werden alle Tastatureingaben aufgezeichnet, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z.B. Anmeldeinformationen oder Kreditkartennummern filtern.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL keylogger

Sprzęt lub oprogramowanie do rejestrowania naciśnięć klawiszy. Wszystkie naciśnięcia klawiszy są rejestrowane w celu przekazania ich atakującemu w sposób możliwie niezauważalny. Atakujący może następnie wykorzystać te informacje do odfiltrowania ważnych dla niego danych, takich jak informacje do logowania lub numery kart kredytowych.

Źródło: Słownikf BSI

LIT Paspaudimų sekiklis

Techninė įranga arba programinė įranga, skirta įrašyti klavišų paspaudimus. Visi klavišų paspaudimai įrašomi taip, kad juos būtų galima nepastebimai perduoti užpuolikui. Tada užpuolikas gali naudoti šią informaciją, kad filtruotų jam svarbius duomenis, pvz., Prisijungimo informaciją ar kredito kortelės numerius.

šaltinis: BSI žodynas

IT keylogger

Hardware o software per la registrazione delle battute. Tutti i tasti premuti vengono registrati in modo che possano essere trasmessi a un aggressore nel modo più inosservato possibile. L'aggressore può quindi utilizzare queste informazioni per filtrare i dati che sono importanti per lui, come le informazioni di login o i numeri di carta di credito.

Fonte: Glossario di BSI

Login/User-ID

The user ID is the name by which the user identifies himself to an IT system. This can be the actual name, a pseudonym, an abbreviation or a combination of letters and/or digits.

Source: Glossary of BSI

DE Benutzerkennung (Benutzerkonto)

Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine Kombination aus Buchstaben und/oder Ziffern.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL Login/Użytkownik-ID

Identyfikator użytkownika to nazwa, za pomocą której użytkownik identyfikuje się w systemie informatycznym. Może to być rzeczywiste nazwisko, pseudonim, skrót lub kombinacja liter i/lub cyfr.

Źródło: Słownikf BSI

LIT Prisijungimas/vartotojo ID

Vartotojo ID yra vardas, kuriuo vartotojas identifikuoja save IT sistemoje. Tai gali būti tikrasis vardas, pseudonimas, santrumpa arba raidžių ir (arba) skaičių derinys.

šaltinis: BSI žodynas

IT Accesso

L'ID utente è il nome con cui l'utente si identifica in un sistema informatico. Può essere il nome vero e proprio, uno pseudonimo, un'abbreviazione o una combinazione di lettere e/o cifre.

Fonte: Glossario di BSI

main memory

The memory of a computer in which all data required for specific work processes are temporarily stored. From there, they can be retrieved and modified later without being changed and are also referred to as "RAM" (Random Access Memory).

Source: Glossary of BSI

DE Arbeitsspeicher

Speicher eines Computers, in dem alle Daten, die für konkrete Arbeitsvorgänge benötigt werden, vorübergehend abgelegt werden. Von dort können sie später unverändert wieder aufgerufen und verändert werden. Wird auch als "RAM" (Random Access Memory) bezeichnet.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL pamięć główna

Pamięć komputera, w której tymczasowo przechowywane są wszystkie dane potrzebne do określonych procesów roboczych. Stamtąd mogą być one później pobierane i modyfikowane bez zmiany i są również określane jako "RAM" (Random Access Memory).

Źródło: Słownikf BSI

LIT Pagrindinė atmintis

Kompiuterio atmintis, kurioje laikinai saugomi visi konkretiems darbo procesams reikalingi duomenys. Iš ten juos vėliau galima paimti ir modifikuoti nekeičiant, jie taip pat vadinami „RAM“ (atsitiktinės prieigos atmintis).

šaltinis: BSI žodynas

IT memoria principale

La memoria di un computer in cui sono immagazzinati temporaneamente tutti i dati necessari per specifici processi di lavoro. Da lì, possono essere recuperati e modificati in seguito senza essere cambiati e sono anche chiamati "RAM" (Random Access Memory).

Fonte: Glossario di BSI

Malware

Software designed with the aim of performing unwanted and usually harmful functions. Examples include computer viruses, worms and Trojan horses. Malicious software is usually designed for a specific operating system variant and is therefore mostly written for common systems and applications.

Source: Glossary of BSI

DE Schadsoftware

Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Quelle: Glossar der Cyber-Sicherheit – BSI

POL złośliwe oprogramowanie

Oprogramowanie zaprojektowane w celu wykonywania niepożądanych i zazwyczaj szkodliwych funkcji. Przykładem są wirusy komputerowe, robaki i konie trojańskie. Złośliwe oprogramowanie jest zwykle projektowane dla konkretnego wariantu systemu operacyjnego i dlatego w większości przypadków jest pisane z myślą o zwykłych systemach i aplikacjach.

Źródło: Słownikf BSI

LIT kenkėjiška programa

Programinė įranga sukurta siekiant atlikti nepageidaujamas ir dažniausiai kenksmingas funkcijas. Pavyzdžiui, kompiuteriniai virusai, kirminai ir Trojos arkliai. Kenkėjiška programinė įranga paprastai yra skirta konkrečiam operacinės sistemos variantui, todėl dažniausiai yra skirta bendroms sistemoms ir programoms.

šaltinis: BSI žodynas

IT malware

Software progettato con lo scopo di eseguire funzioni indesiderate e solitamente dannose. Gli esempi includono virus informatici, worm e cavalli di Troia. Il software dannoso è di solito progettato per una specifica variante del sistema operativo e quindi è per lo più scritto per sistemi e applicazioni comuni.

Fonte: Glossario di BSI

mobile IT system

IT system whose intended use is characterized by mobility mobility. Typical mobile IT systems are, for example, notebooks, smartphones, tablets or digital cameras.

Source: VDS 10000

DE Mobiles IT-System

IT-System, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile IT-Systeme sind z. B. Notebooks, Smartphones, Tablets oder Digitalkameras.

Quelle: VDS 10000

POL mobilny system informatyczny

System informatyczny, którego przeznaczenie charakteryzuje się mobilnością. Typowe mobilne systemy informatyczne to na przykład notebooki, smartfony, tablety czy aparaty cyfrowe.

Źródło: VDS 10000

LIT mobilioji IT sistema

IT sistema, kurios paskirtis yra mobilumas. Įprastos mobiliosios IT sistemos yra, pavyzdžiui, nešiojamieji kompiuteriai, išmanieji telefonai, planšetiniai kompiuteriai ar skaitmeniniai fotoaparatai.

šaltinis: VSD 10000

IT sistema informatico mobile

Sistema IT la cui destinazione d'uso è caratterizzata dalla mobilità. Tipici sistemi IT mobili sono, per esempio, notebook, smartphone, tablet o fotocamere digitali.

Fonte: VDS 10000

operating system

Operating systems are the most crucial programs. Without them, a computer does not run. They are loaded first when starting (booting) e.g. a computer or smartphone. Other programs use the operating system as a basis. Available operating systems for computers are, for example, DOS, Windows, Mac OS or Linux. For smartphones for example Android, iOS, Windows Phone or Blackberry OS.

Source: Glossary of BSI

DE Betriebssystem

Betriebssysteme sind die wichtigsten Programme. Ohne sie läuft ein Computer nicht. Sie werden beim Start (Booten) z.B. eines Computers oder Smartphone zuerst geladen. Andere Programme nutzen das Betriebssystem als Grundlage. Bekannte Betriebssysteme für Computer sind beispielsweise DOS, Windows, Mac OS oder Linux. Bei Smartphones sind es z.B. Android, iOS, Windows Phone oder Blackberry-OS.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL system operacyjny

Systemy operacyjne są najważniejszymi programami. Bez nich komputer nie działa. Są one ładowane jako pierwsze podczas uruchamiania (bootowania) np. komputera lub smartfona. Inne programy korzystają z systemu operacyjnego jako podstawy. Dostępne systemy operacyjne dla komputerów to np. DOS, Windows, Mac OS lub Linux. W przypadku smartfonów są to na przykład Android, iOS, Windows Phone lub Blackberry OS.

Źródło: Słownikf BSI

LIT Operacinė sistema

Operacinės sistemos yra svarbiausios programos. Be jų kompiuteris neveikia. Jos pirmiausia įkeliamos paleidžiant (paleidžiant) pvz. kompiuterį ar išmanųjį telefoną. Kitos programos naudoja operacinę sistemą. Galimos kompiuterių operacinės sistemos, pavyzdžiui, DOS, „Windows", „Mac OS" ar „Linux". Išmaniesiems telefonams, pvz., „Android", „iOS", „Windows Phone" ar „Blackberry OS".

šaltinis: BSI žodynas

IT sistema operativo

I sistemi operativi sono i programmi più importanti. Senza di loro, un computer non funziona. Vengono caricati per primi quando si avvia (booting) ad esempio un computer o uno smartphone. Altri programmi usano il sistema operativo come base. I sistemi operativi disponibili per i computer sono, per esempio, DOS, Windows, Mac OS o Linux. Per gli smartphone per esempio Android, iOS, Windows Phone o Blackberry OS.

Fonte: Glossario di BSI

pharming

As with phishing, access data is usually the target of an attack in pharming. The difference to phishing is that in pharming, the infrastructure is manipulated in such a way that the victim ends up on a fake website even if he has entered the correct address of the service.

Source: Glossary of BSI

DE Pharming

Wie beim Phishing sind auch beim Pharming meist Zugangsdaten das Ziel eines Angriffs. Der Unterschied zum Phishing besteht darin, dass beim Pharming die Infrastruktur so manipuliert wird, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn er die korrekte Adresse des Dienstes eingeben hat.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL pharming

Podobnie jak w przypadku phishingu, celem ataku w pharmingu są zazwyczaj dane dostępowe. Różnica w stosunku do phishingu polega na tym, że w pharmingu infrastruktura jest zmanipulowana w taki sposób, że ofiara trafia na fałszywą stronę, nawet jeśli wpisała prawidłowy adres serwisu.

Źródło: Słownikf BSI

LIT farmingas

Kaip ir sukčiavimo atveju, prieigos duomenys dažniausiai yra atakos tikslas. Skirtumas nuo sukčiavimo yra tas, kad sukčiavimo metu infrastruktūra manipuliuojama taip, kad auka atsiduria netikroje svetainėje, net jei įvedė teisingą paslaugos adresą.

šaltinis: BSI žodynas

IT pharming

Come nel phishing, i dati di accesso sono di solito l'obiettivo di un attacco nel pharming. La differenza rispetto al phishing è che nel pharming, l'infrastruttura viene manipolata in modo tale che la vittima finisca su un sito web falso anche se ha inserito l'indirizzo corretto del servizio.

Fonte: Glossario di BSI

phising

The word is a combination of "password" and "fishing". Phishing is an attempt to obtain access data for a service or website, for example, by means of fake e-mails and/or websites.

Source: Glossary of BSI

DE Phising

Das Wort setzt sich aus "Password" und "Fishing" zusammen, zu Deutsch "nach Passwörtern angeln". Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL phising

Słowo to jest połączeniem słów "password" i "fishing". Phishing to próba uzyskania danych dostępowych do serwisu lub strony internetowej, np. za pomocą fałszywych e-maili i/lub stron internetowych.

Źródło: Słownikf BSI

LIT sukčiavimas

Žodis yra „slaptažodžio" ir „žvejybos" derinys. Sukčiavimas yra bandymas gauti prieigos prie paslaugos ar svetainės duomenis, pavyzdžiui, naudojant suklastotus el. laiškus ir (arba) svetaines.

šaltinis: BSI žodynas

IT phising

La parola è una combinazione di "password" e "fishing". Il phishing è un tentativo di ottenere dati di accesso per un servizio o un sito web, per esempio, per mezzo di false e-mail e wibsites

Fonte: Glossario di BSI

poisoning

Injection of manipulated data into a cache, which is then used by other applications or services. Examples are attacks using poisoning on DNS, BGP, or ARP caches. An attacker can, for example, generally change the routes of data packets or redirect specific requests for a bank's web pages to a fake page.

Source: Glossary of BSI

DE Poisoning

Einschleusen von manipulierten Daten in einen Zwischenspeicher (Cache), der dann von anderen Anwendungen oder Diensten genutzt wird. Beispiele sind Angriffe mittels Poisoning auf DNS-, BGP-, oder ARP-Caches. Ein Angreifer kann so z.B. allgemein die Routen von Datenpaketen ändern oder gezielt Anfragen für Webseiten einer Bank auf eine gefälschte Seite umleiten.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL poisoning

Wstrzykiwanie zmanipulowanych danych do pamięci podręcznej, które są następnie wykorzystywane przez inne aplikacje lub usługi. Przykładem mogą być ataki wykorzystujące zatruwanie pamięci podręcznej DNS, BGP lub ARP. Atakujący może np. ogólnie zmienić trasy pakietów danych lub przekierować określone żądania dotyczące stron internetowych banku na fałszywą stronę.

Źródło: Słownikf BSI

LIT nuodijimas

Manipuliuotų duomenų įvedimas į talpyklą, kurią vėliau naudoja kitos programos ar paslaugos. Pavyzdžiai yra išpuoliai, naudojant apsinuodijimą DNS, BGP arba ARP talpyklose. Pavyzdžiui, užpuolikas gali paprastai pakeisti duomenų paketų maršrutus arba nukreipti konkrečias banko tinklalapių užklausas į suklastotą puslapį.

šaltinis: BSI žodynas

IT avvelenamento

Iniezione di dati manipolati in una cache, che viene poi utilizzata da altre applicazioni o servizi. Esempi sono gli attacchi che utilizzano l'avvelenamento delle cache DNS, BGP o ARP. Un attaccante può, per esempio, cambiare generalmente i percorsi dei pacchetti di dati o reindirizzare specifiche richieste per le pagine web di una banca a una pagina falsa.

Fonte: Glossario di BSI

risk management

The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.

Source: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

DE Risikomanagement

Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL zarządzanie ryzykiem

Proces, różniący się od oceny ryzyka, polegający na rozważeniu alternatywnych rozwiązań strategicznych w porozumieniu z zainteresowanymi stronami, uwzględniający ocenę ryzyka i inne uzasadnione czynniki oraz wybierający odpowiednie opcje zapobiegania i kontroli.

Źródło: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

LIT rizikos valdymas

Procesas, kuris skiriasi nuo rizikos vertinimo, sveriant politikos alternatyvas, konsultuojantis su suinteresuotosiomis šalimis, atsižvelgiant į rizikos vertinimą ir kitus teisėtus veiksnius bei pasirenkant tinkamas prevencijos ir kontrolės galimybes.

šaltinis: BSI žodynas

IT gestione del rischio

Il processo, distinto dalla valutazione del rischio, di soppesare le alternative politiche in consultazione con le parti interessate, considerando la valutazione del rischio e altri fattori legittimi, e selezionando le opzioni di prevenzione e controllo appropriate.

Fonte: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

scareware

Scareware is a form of malware that users install on their systems themselves. In most cases, the user is led to believe that there is a problem with their computer while surfing the Internet by deceiving them or exploiting their technical lack of understanding. Often, an infection with malware is reported, an alleged malfunction of the operating system is detected or an important security update is advertised. If a user trusts these messages and installs the offered software, he himself has infected the system with malware in the worst case.

Source: Glossary of BSI

DE Scareware

Scareware ist eine Form von Schadsoftware, die der Nutzer selbst auf seinem System installiert. In den meisten Fällen wird dem Nutzer beim Surfen im Internet durch Täuschung oder Ausnutzen von technischem Unverständnis suggeriert, dass ein Problem mit seinem Computer besteht. Häufig wird dazu eine Infektion mit Schadsoftware gemeldet, eine angebliche Fehlfunktion des Betriebssystems erkannt oder mit einem wichtigen Sicherheits-Update geworben. Vertraut ein Anwender auf diese Meldungen und installiert die angebotene Software, hat er selbst dadurch das System im ungünstigsten Fall mit einer Schadsoftware infiziert.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL scareware

Scareware to forma złośliwego oprogramowania, które użytkownicy sami instalują w swoich systemach. W większości przypadków użytkownik jest przekonany o istnieniu problemu z komputerem podczas surfowania po Internecie poprzez wprowadzenie go w błąd lub wykorzystanie jego braku wiedzy technicznej. Często zgłaszana jest infekcja złośliwym oprogramowaniem, wykrywana jest rzekoma usterka systemu operacyjnego lub reklamowana jest ważna aktualizacja zabezpieczeń. Jeśli użytkownik zaufa tym wiadomościom i zainstaluje oferowane oprogramowanie, w najgorszym przypadku sam zainfekował system złośliwym oprogramowaniem.

Źródło: Słownikf BSI

LIT kenkėjiška programa

„Scareware" yra kenkėjiškų programų forma, kurią vartotojai patys diegia savo sistemose. Daugeliu atvejų vartotojas yra įsitikinęs, kad naršant internete kyla problemų dėl jo kompiuterio, jį apgaudinėjant ar pasinaudojant techniniu nesupratimu. Dažnai pranešama apie kenkėjiškų programų užkrėtimą, aptinkamas tariamas operacinės sistemos veikimo sutrikimas arba reklamuojamas svarbus saugos naujinimas. Jei vartotojas pasitiki šiais pranešimais ir įdiegia siūlomą programinę įrangą, jis pats blogiausiu atveju užkrėtė sistemą kenkėjiška programa.

šaltinis: BSI žodynas

IT scareware

Lo scareware è una forma di malware che gli utenti stessi installano sui loro sistemi. Nella maggior parte dei casi, l'utente è portato a credere che ci sia un problema con il suo computer mentre naviga in Internet, ingannandolo o sfruttando la sua mancanza di comprensione tecnica. Spesso viene segnalata un'infezione da malware, viene rilevato un presunto malfunzionamento del sistema operativo o viene pubblicizzato un importante aggiornamento di sicurezza. Se un utente si fida di questi messaggi e installa il software offerto, nel peggiore dei casi ha infettato lui stesso il sistema con un malware.

Fonte: Glossario di BSI

secret keys

Secret keys are used in the context of symmetric cryptoalgorithms. Unlike the private keys used in asymmetric cryptoalgorithms, the entire key material is known to all communication partners.

Source: Glossary of BSI

DE Geheime Schlüssel

Geheime Schlüssel werden im Zusammenhang mit symmetrischen Kryptoalgorithmen verwendet. Im Gegensatz zu den bei asymmetrischen Kryptoalgorithmen eingesetzten privaten Schlüsseln ist das gesamte Schlüsselmaterial allen Kommunikationspartnern bekannt.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL tajne klucze

Tajne klucze są używane w kontekście kryptowalut symetrycznych. W przeciwieństwie do kluczy prywatnych stosowanych w kryptowalutach asymetrycznych, cały materiał klucza jest znany wszystkim partnerom komunikacji.

Źródło: Słownikf BSI

LIT slaptieji raktai

Slaptieji raktai naudojami simetrinių kriptoalgoritmų kontekste. Skirtingai nuo asimetriniuose kriptoalgoritmuose naudojamų privačių raktų, visa pagrindinė medžiaga yra žinoma visiems komunikacijos partneriams.

šaltinis: BSI žodynas

IT chiavi segrete

Le chiavi segrete sono utilizzate nel contesto dei crittoalgoritmi simmetrici. A differenza delle chiavi private utilizzate nei crittoalgoritmi asimmetrici, l'intero materiale della chiave è noto a tutti i partner di comunicazione.

Fonte: Glossario di BSI

security concept

A security concept is used to implement the security strategy and describes the planned procedure for achieving the security goals set for an institution. The security concept is the central document in the security process of a company or an authority. Every concrete security measure must ultimately be traceable to it.

Source: Glossary of BSI

DE Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL koncepcja bezpieczeństwa

Koncepcja bezpieczeństwa jest wykorzystywana do wdrażania strategii bezpieczeństwa i opisuje planowaną procedurę osiągania celów bezpieczeństwa wyznaczonych dla danej instytucji. Koncepcja bezpieczeństwa jest centralnym dokumentem w procesie bezpieczeństwa firmy lub instytucji. Każdy konkretny środek bezpieczeństwa musi być ostatecznie do niej przyporządkowany.

Źródło: Słownikf BSI

LIT saugumo koncepcija

Saugumo koncepcija naudojama saugumo strategijai įgyvendinti ir apibūdina planuojamą įstaigai iškeltų saugumo tikslų įgyvendinimo tvarką. Saugumo koncepcija yra pagrindinis dokumentas įmonės ar institucijos saugumo procese. Galų gale kiekviena konkreti saugumo priemonė turi būti atsekama.

šaltinis: BSI žodynas

IT concetto di sicurezza

Un concetto di sicurezza è usato per implementare la strategia di sicurezza e descrive la procedura pianificata per raggiungere gli obiettivi di sicurezza stabiliti per un'istituzione. Il concetto di sicurezza è il documento centrale nel processo di sicurezza di un'azienda o di un'autorità. Ogni misura di sicurezza concreta deve alla fine essere riconducibile ad esso.

Fonte: Glossario di BSI

security requirements

Security requirements are requirements for the organizational, personnel, infrastructural and technical areas, the fulfillment of which is necessary to increase information security or contributes to it. A security requirement therefore describes what must be done to achieve a certain level of information security.

Source: Glossary of BSI

DE Sicherheitsanforderungen

Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL wymogi bezpieczeństwa

Wymogi bezpieczeństwa to wymagania dotyczące obszarów: organizacyjnego, personalnego, infrastrukturalnego i technicznego, których spełnienie jest niezbędne do zwiększenia bezpieczeństwa informacji lub przyczynia się do jego zwiększenia. Wymogi bezpieczeństwa opisują zatem, co należy zrobić, aby osiągnąć określony poziom bezpieczeństwa informacji.

Źródło: Słownikf BSI

LIT saugumo reikalavimai

Saugumo reikalavimai - tai reikalavimai organizacinėms, personalo, infrastruktūros ir techninėms sritims, kurių įvykdymas yra būtinas siekiant padidinti informacijos saugumą arba prisidėti prie jo. Todėl saugumo reikalavime aprašoma, ką reikia padaryti norint pasiekti tam tikrą informacijos saugumo lygį.

šaltinis: BSI žodynas

IT requisiti di sicurezza

I requisiti di sicurezza sono requisiti per l'area organizzativa, personale, infrastrutturale e tecnica, il cui adempimento è necessario per aumentare la sicurezza delle informazioni o vi contribuisce. Un requisito di sicurezza descrive quindi ciò che deve essere fatto per raggiungere un certo livello di sicurezza delle informazioni.

Fonte: Glossario di BSI

social engineering

In cyber-attacks using social engineering, criminals try to entice their victims to disclose data on their own, bypass protective measures or install malware on their systems on their own. In both cybercrime and espionage, the criminals take a clever approach to exploit supposed human weaknesses such as curiosity or fear in order to gain access to sensitive data and information.

Source: Glossary of BSI

DE Social Engineering

Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL inżynieria społeczna

W cyberatakach wykorzystujących socjotechnikę przestępcy próbują nakłonić swoje ofiary do samodzielnego ujawnienia danych, obejścia środków ochronnych lub samodzielnego zainstalowania w systemie złośliwego oprogramowania. Zarówno w cyberprzestępczości, jak i w szpiegostwie, przestępcy w sprytny sposób wykorzystują rzekome ludzkie słabości, takie jak ciekawość czy strach, aby uzyskać dostęp do wrażliwych danych i informacji.

Źródło: Słownikf BSI

LIT socialinė inžinerija

Kibernetinėse atakose, naudojant socialinę inžineriją, nusikaltėliai bando privilioti savo aukas savarankiškai atskleisti duomenis, apeiti apsaugos priemones arba patys įdiegti kenkėjiškas programas. Tiek elektroninių nusikaltimų, tiek šnipinėjimo metu nusikaltėliai sumaniai išnaudoja tariamas žmogaus silpnybes, tokias kaip smalsumas ar baimė, siekdami gauti prieigą prie neskelbtinų duomenų ir informacijos.

šaltinis: BSI žodynas

IT ingegneria sociale

Negli attacchi informatici che utilizzano l'ingegneria sociale, i criminali cercano di invogliare le loro vittime a rivelare dati per conto proprio, a bypassare le misure di protezione o a installare malware sui loro sistemi per conto proprio. Sia nel cybercrimine che nello spionaggio, i criminali adottano un approccio intelligente per sfruttare presunte debolezze umane come la curiosità o la paura, al fine di ottenere l'accesso a dati e informazioni sensibili.

Fonte: Glossario di BSI

spoofing

In information technology, spoofing is the name given to various attempts to conceal one's own identity and to forge transmitted data. The aim is to undermine the integrity and authenticity of information processing.

Source: Glossary of BSI

DE Spoofing

Spoofing nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL spoofing

W informatyce spoofing to nazwa nadana różnym próbom ukrycia własnej tożsamości i fałszowania przesyłanych danych. Celem jest podważenie integralności i autentyczności przetwarzania informacji.

Źródło: Słownikf BSI

LIT sukčiavimas

Informacinėse technologijose sukčiavimas vadinamas įvairiais bandymais nuslėpti savo tapatybę ir suklastoti perduotus duomenis. Tikslas yra pakenkti informacijos apdorojimo vientisumui ir autentiškumui.

šaltinis: BSI žodynas

IT spoofing

Nella tecnologia dell'informazione, lo spoofing è il nome dato ai vari tentativi di nascondere la propria identità e di falsificare i dati trasmessi. Lo scopo è quello di minare l'integrità e l'autenticità del trattamento delle informazioni.

Fonte: Glossario di BSI

spyware

Spyware refers to programs that secretly, i.e. without indicating it, collect information about a user or the use of a computer and forward it to the creator of the spyware. Spyware is often considered just a nuisance, but it should not be overlooked that spyware can also be used to obtain security-related information such as passwords.

Source: Glossary of BSI

DE Spyware

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL spyware

Oprogramowanie szpiegujące to programy, które potajemnie, tj. bez wskazywania na to, zbierają informacje o użytkowniku lub korzystaniu z komputera i przekazują je do twórcy oprogramowania szpiegującego. Oprogramowanie szpiegujące jest często uważane za uciążliwe, ale nie należy zapominać, że może być również używane do pozyskiwania informacji związanych z bezpieczeństwem, takich jak hasła.

Źródło: Słownikf BSI

LIT šnipinėjimo programos

Šnipinėjimo programos reiškia programas, kurios slaptai, t. Y. Nenurodydamos, renka informaciją apie vartotoją ar kompiuterio naudojimą ir perduoda ją šnipinėjimo programos kūrėjui. Šnipinėjimo programos dažnai laikomos tik nepatogumais, tačiau nereikėtų pamiršti, kad šnipinėjimo programos taip pat gali būti naudojamos su saugumu susijusiai informacijai, pavyzdžiui, slaptažodžiams gauti.

šaltinis: BSI žodynas

IT spyware

Lo spyware si riferisce a programmi che segretamente, cioè senza indicarlo, raccolgono informazioni su un utente o sull'uso di un computer e le inoltrano al creatore dello spyware. Lo spyware è spesso considerato solo una seccatura, ma non bisogna trascurare che lo spyware può anche essere usato per ottenere informazioni relative alla sicurezza, come le password.

Fonte: Glossario di BSI

threat

Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Source: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

DE Bedrohung

Ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL zagrożenie

Wszelkie okoliczności lub zdarzenia, które mogą mieć negatywny wpływ na aktywa poprzez nieautoryzowany dostęp, zniszczenie, ujawnienie, modyfikację danych i/lub odmowę usługi.

Źródło: Słownikf BSI

LIT grėsmė

Bet kokios aplinkybės ar įvykiai, galintys neigiamai paveikti turtą neteisėtai prieinant, sunaikinant, atskleidžiant, keičiant duomenis ir (arba) atsisakant paslaugų.

šaltinis: BSI žodynas

IT minaccia

Qualsiasi circostanza o evento con il potenziale di avere un impatto negativo su una risorsa attraverso l'accesso non autorizzato, la distruzione, la divulgazione, la modifica dei dati e/o la negazione del servizio.

Fonte: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

traceroute/pathping

A program to find out over which routers data is sent to a remote computer. As a result, the program provides a route description of the data packets, so to speak, and information about the time needed for this route.

Source: Glossary of BSI

DE Traceroute/Pathping

Ein Programm, um herauszufinden, über welche Router Daten zu einem entfernten Rechner gesandt werden. Als Ergebnis liefert das Programm sozusagen eine Wegbeschreibung der Datenpakete und Angaben über die für diesen Weg benötigte Zeit.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL traceroute/pathping

Program do sprawdzania, przez jakie routery przesyłane są dane do zdalnego komputera. W rezultacie program podaje opis trasy pakietów danych oraz informację o czasie potrzebnym na przebycie tej trasy.

Źródło: Słownikf BSI

LIT maršruto sekiklis

Programa, skirta sužinoti, kurie maršrutizatoriaus duomenys siunčiami į nuotolinį kompiuterį. Dėl to programa pateikia duomenų paketų maršruto aprašymą, taip sakant, ir informaciją apie laiką, reikalingą šiam maršrutui.

šaltinis: BSI žodynas

IT traceroute

Un programma per scoprire attraverso quali router i dati vengono inviati a un computer remoto. Come risultato, il programma fornisce una descrizione del percorso dei pacchetti di dati, per così dire, e informazioni sul tempo necessario per questo percorso.

Fonte: Glossario di BSI

transport encryption

Transport encryption (e.g., with TLS) is point-to-point encryption. In the case of the e-mail application, the content is encrypted during transmission between the sender and its e-mail provider and between two e-mail providers and between the e-mail provider and the recipient. The process is automated and usually requires no action by the sender or recipient.

Source: Glossary of BSI

DE Transportverschlüsselung

Die Transportverschlüsselung (z.B. mit TLS) ist eine Punkt-zu-Punkt-Verschlüsselung. Bei der E-Mail-Anwendung wird der Inhalt bei der Übermittlung zwischen dem Absender und seinem E-Mail-Anbieter sowie zwischen zwei E-Mail-Anbietern untereinander und zwischen E-Mail-Anbieter und Empfänger verschlüsselt. Der Prozess läuft automatisiert ab und verlangt in der Regel keine Aktion des Absenders oder Empfängers.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL szyfrowanie transportu

Szyfrowanie transportowe (np. za pomocą TLS) jest szyfrowaniem typu point-to-point. W przypadku aplikacji poczty elektronicznej treść jest szyfrowana podczas transmisji między nadawcą a jego dostawcą poczty elektronicznej oraz między dwoma dostawcami poczty elektronicznej i między dostawcą poczty elektronicznej a odbiorcą. Proces ten jest zautomatyzowany i zazwyczaj nie wymaga żadnych działań ze strony nadawcy lub odbiorcy.

Źródło: Słownikf BSI

LIT transporto šifravimas

Transporto šifravimas (pvz., Naudojant TLS) yra šifravimas iš vieno taško į kitą. El. Pašto programos atveju turinys užšifruojamas perduodant siuntėją ir jo el. Pašto teikėją, tarp dviejų el. Pašto paslaugų teikėjų ir tarp el. Pašto teikėjo bei gavėjo. Procesas yra automatizuotas ir paprastai nereikalauja siuntėjo ar gavėjo veiksmų.

šaltinis: BSI žodynas

IT crittografia del trasporto

La crittografia del trasporto (per esempio, con TLS) è una crittografia punto a punto. Nel caso dell'applicazione e-mail, il contenuto viene criptato durante la trasmissione tra il mittente e il suo provider di posta elettronica e tra due provider di posta elettronica e tra il provider di posta elettronica e il destinatario. Il processo è automatizzato e di solito non richiede alcuna azione da parte del mittente o del destinatario.

Fonte: Glossario di BSI

two-factor authentication

Two-factor authentication refers to the combination of two factors from the three areas of knowledge (e.g., password), possession (e.g., smart card), and biometrics (e.g., fingerprint).

Source: Glossary of BSI

DE Zwei-Faktor-Authentisierung

Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Faktoren aus den drei Bereichen Wissen (z.B. Passwort), Besitz (z.B. Chipkarte) und Biometrie (z.B. Fingerabdruck).

Quelle: Glossar der Cyber-Sicherheit - BSI

POL uwierzytelnianie dwuskładnikowe

Uwierzytelnianie dwuskładnikowe odnosi się do kombinacji dwóch czynników z trzech obszarów: wiedzy (na przykład hasło), posiadania (na przykład karta inteligentna) i biometrii (na przykład odcisk palca).

Źródło: Słownikf BSI

LIT dviejų veiksnių autentifikavimas

Dviejų veiksnių autentifikavimas reiškia dviejų veiksnių derinį iš trijų žinių sričių (pvz., slaptažodžio), turėjimo (pavyzdžiui, išmanioji kortelė) ir biometrinių duomenų (pvz., pirštų atspaudų).

šaltinis: BSI žodynas

IT autenticazione a due fattori

L'autenticazione a due fattori si riferisce alla combinazione di due fattori dalle tre aree della conoscenza (per esempio, la password), del possesso (per esempio, la smart card) e della biometria (per esempio, l'impronta digitale).

Fonte: Glossario di BSI

virtual private network

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

Source: What Is a VPN? - Virtual Private Network - Cisco

DE Virtuelle Private Netze (VPN)

VPN steht für Virtual Private Network. Es verschlüsselt die Datenkommunikation zwischen zwei Endpunkten – zum Beispiel zwischen einem Endgerät und einem VPN-Server. Auf diese Weise kann die Kommunikation nicht ohne weiteres mitgelesen oder verändert werden.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL wirtualna sieć prywatna

Wirtualna sieć prywatna, czyli VPN, to szyfrowane połączenie przez Internet z urządzenia do sieci. Szyfrowane połączenie pomaga zapewnić bezpieczne przesyłanie poufnych danych. Zapobiega podsłuchiwaniu ruchu przez osoby nieupoważnione i pozwala użytkownikowi na zdalne wykonywanie pracy. Technologia VPN jest szeroko stosowana w środowiskach korporacyjnych.

Źródło: What Is a VPN? - Virtual Private Network - Cisco

LIT Virtualus privatus tinklas

Virtualus privatus tinklas arba VPN yra užšifruotas ryšys internetu iš įrenginio į tinklą. Užšifruotas ryšys padeda užtikrinti, kad neskelbtini duomenys būtų saugiai perduodami. Tai neleidžia pašaliniams asmenims klausytis eismo ir leidžia vartotojui dirbti nuotoliniu būdu. VPN technologija plačiai naudojama verslo aplinkoje.

šaltinis: BSI žodynas

IT rete privata virtuale

Una rete privata virtuale, o VPN, è una connessione criptata su Internet da un dispositivo a una rete. La connessione criptata aiuta a garantire che i dati sensibili siano trasmessi in modo sicuro. Impedisce alle persone non autorizzate di origliare il traffico e permette all'utente di lavorare in remoto. La tecnologia VPN è ampiamente utilizzata negli ambienti aziendali.

Fonte: Cos'è una VPN? - Rete privata virtuale - Cisco

viruses

Classic form of malicious software that spreads itself and can carry different malicious potential (no malicious function up to deletion of data on a hard disk). Viruses occur in combination with a host, e.g. an infected document or program.

Source: Glossary of BSI

DE Viren

Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). Viren treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL wirusy

Klasyczna forma złośliwego oprogramowania, które rozprzestrzenia się samoczynnie i może nieść ze sobą różny potencjał złośliwości (bez funkcji złośliwych aż do kasowania danych na dysku twardym). Wirusy występują w połączeniu z gospodarzem, np. zainfekowanym dokumentem lub programem.

Źródło: Słownikf BSI

LIT virusai

Klasikinė kenkėjiškos programinės įrangos forma, kuri plinta pati ir gali turėti skirtingą kenkėjišką potencialą (be kenkėjiškų funkcijų iki duomenų ištrynimo kietajame diske). Virusai atsiranda kartu su šeimininku, pvz. užkrėstą dokumentą ar programą.

šaltinis: BSI žodynas

IT virus

Classica forma di software maligno che si diffonde da solo e può portare diversi potenziali maligni (nessuna funzione maligna fino alla cancellazione di dati su un disco rigido). I virus si presentano in combinazione con un ospite, ad esempio un documento o un programma infetto.

Fonte: Glossario di BSI

worm

(Computer, Internet, e-mail) worms are malicious software, similar to a virus, which reproduces itself and spreads independently by exploiting communication interfaces.

Source: Glossary of BSI

DE Wurm

Bei (Computer-, Internet-, E-Mail-)Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.

Quelle: Glossar der Cyber-Sicherheit - BSI

POL robaki

(Komputer, Internet, e-mail) robaki to złośliwe oprogramowanie, podobne do wirusa, które samo się rozmnaża i rozprzestrzenia samodzielnie, wykorzystując interfejsy komunikacyjne.

Źródło: Słownikf BSI

LIT kirminas

(Kompiuterio, interneto, el. pašto) kirminai yra kenkėjiška programinė įranga, panaši į virusą, kuri dauginasi ir savarankiškai plinta naudodama ryšio sąsajas.

šaltinis: BSI žodynas

IT verme

I worm (computer, Internet, e-mail) sono software maligni, simili a un virus, che si riproducono e si diffondono autonomamente sfruttando le interfacce di comunicazione.

Fonte: Glossario di BSI