UGCS301VAT

سائبر سیکیورٹی

(Cyber Security)

بی۔اے۔/بی۔کام۔/بی۔ایس سی۔(آنرس)

چار سالہ پروگرام

تیسرا سمسٹر (ویلیو ایڈیڈ کورس)

مرکز برائے فاصلاتی و آن لائن تعلیم

مولانا آزاد نیشنل اردو یونیورسٹی

حیدرآباد۔32، تلنگانہ، بھارت

Copyright © 2025, Maulana Azad National Urdu University, Hyderabad
All right reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronically or mechanically, including photocopying, recording or any information storage or retrieval system, without prior permission in writing form the publisher (registrar@manuu.edu.in)

ISBN : 978-81-68324-35-0
Course : Cyber Security
First Edition : September 2026
Copies : 7500
Price : 160/- (The price of the book is included in admission fee of distance mode students)

Course Coordinator

Prof. Pradeep Kumar, Professor and Head, CS&IT

Editorial Board/Editors

Prof. Pradeep Kumar,
Professor and Head,
CS&IT, MANUU.

Jameel Ahamed,
Assistant professor,
CS&IT, MANUU

Khaleda Afroz,
Assistant professor,
CS&IT, MANUU

Dr. Khaleel Ahmed,
Asst. professor,
CS&IT, MANUU

Alisha Raza,
Assistant professor (C),
CS&IT, MANUU

Md Nadeem Noori,
Assistant professor (C),
CS&IT, MANUU

Dr. Sobiya Arsheen
(Language Editor)

Production

Prof. Nikhath Jahan,
Professor (Urdu),
CDOE MANUU

Mr. P Habibulla
Assistant Registrar, Purchase & Stores Section, MANUU

Dr. Mohd Akmal Khan,
Assistant Professor (C),
CDOE MANUU

Mohd Abdul Naseer
Section Officer, CDOE MANUU

Shaik Ismail,
UDC, CDOE, MANUU

Syed Faheemuddin, LDC
Purchase & Stores Section, MANUU

On behalf of the Registrar, Published by:
Centre for Distance and Online Education
Maulana Azad National Urdu University
Gachibowli, Hyderabad-500032 (TG), India
Director: dir.dde@manuu.edu.in; *Publication:* ddepublication@manuu.edu.in
Phone number: 040-23008314; Website: manuu.edu.in

CRC Prepared by the Ibrahim Akram Siddique (DEO), CDOE, MANUU

Printed at: Print Time & Business Enterprises, Hyderabad

فہرست

پیغام	وائس چانسلر، مولانا آزاد نیشنل اردو یونیورسٹی	5
پیغام	ڈائرکٹر، مرکز برائے فاصلاتی و آن لائن تعلیم	6
کورس کا تعارف	پروگرام کوآرڈینیٹر	7

اکائی نمبر	اکائی کا نام	مصنف	صفحہ نمبر
بلاک I			
1۔	سائبر سیکیورٹی	علیشار ضا	9
2۔	سائبر حملے اور سیکیورٹی پالیسیاں		23
3۔	سائبر جرائم اور روک تھام		35
4۔	سائبر اسپیس اور قانون اور سائبر فورینسکس		44
بلاک II			
5۔	سائبر کرائم: موبائل اور وائرلیس ڈیوایسز	علیشار ضا	61
6۔	سائبر سیکیورٹی: تنظیمی اثرات		77
7۔	رازداری کے مسائل اور سائبر کرائم		86

مصنفین کی تفصیلات

(Writer's Details)

Name and Designation	نام اور عہدہ
Alisha Raza Asst. Professor (Contractual), CS&IT, MANUU	**علیشا رضا** اسسٹنٹ پروفیسر (کانٹریکچویل)، سی ایس اینڈ آئی ٹی، مانو

پروف ریڈرس (Proofreaders):

- **محمد شمس الدین عادل**، سی ایس اینڈ آئی ٹی، مانو

ٹائٹل پیج (Title Page):

- **ابراہیم اکرم صدیقی** (ڈی ای او)، سی ڈی او ای، مانو

پیغام

مولانا آزاد نیشنل اردو یونیورسٹی (MANUU) 1998 میں پارلیمنٹ کے ایک ایکٹ کے ذریعے قائم کی گئی۔ یہ ایک مرکزی جامعہ ہے جس نے این اے اے سی کی جانب سے گریڈ +A حاصل کیا ہے۔ اس جامعہ کے قیام کے مقاصد ہیں: (1) اردو زبان کا فروغ، (2) پیشہ ورانہ اور تکنیکی تعلیم کو اردو میڈیم میں قابل رسائی اور دستیاب بنانا، (3) روایتی اور فاصلاتی طریقۂ تعلیم کے ذریعے تعلیم فراہم کرنا، اور (4) خواتین کی تعلیم پر خصوصی توجہ دینا۔ یہ وہ نکات ہیں جو اس مرکزی جامعہ کو دیگر تمام مرکزی جامعات سے ممتاز کرتے ہیں اور اسے ایک انفرادیت بخشتے ہیں۔ قومی تعلیمی پالیسی 2020 میں بھی مادری زبانوں اور علاقائی زبانوں میں تعلیم حاصل کرنے پر زور دیا گیا ہے۔

اردو کے ذریعے علم کے فروغ کا مقصد یہی ہے کہ اردو جاننے والے طبقے کے لیے عصری علوم اور مضامین تک رسائی آسان بنائی جائے۔ ایک طویل عرصے تک اردو میں درسی مواد کی کمی رہی ہے۔ اردو یونیورسٹی کے پاس اب اردو میں 500 سے زیادہ کتابوں کا ذخیرہ موجود ہے اور ہر سمسٹر کے ساتھ اس تعداد میں اضافہ ہو رہا ہے۔

اردو یونیورسٹی این ای پی 2020 کے وژن کے مطابق مادری/گھریلو زبان میں تعلیمی مواد فراہم کرنے کے قومی مشن کا حصہ بننے کو اپنے لیے ایک اعزاز سمجھتی ہے۔ مزید یہ کہ اردو بولنے والا طبقہ اردو میں مطالعہ کے مواد کی عدم دستیابی کے سبب نئے اُبھرتے شعبوں اور جدید تر معلومات کے موجودہ میدانوں میں تازہ ترین معلومات واطلاعات کے حصول سے محروم نہیں رہے گا۔ مذکورہ بالا میدانوں میں مواد کی دستیابی کی بدولت حصولِ معلومات کا نیا شعور بیدار ہوا ہے جو یقیناً اردو داں طبقے کی دانشورانہ ترقی پر اثر انداز ہوگا۔

فاصلاتی اور آن لائن طلبہ کے لیے تعلیم وتدریس کے عمل کو سہل بنانے کے لیے یونیورسٹی کا سینٹر فار ڈسٹنس اینڈ آن لائن ایجوکیشن (CDOE) اردو اور متعلقہ مضامین میں خود اکتسابی مواد (SLM) کی تیاری کو یقینی بناتا ہے۔

MANUU فاصلاتی اور آن لائن لرننگ کے طلبہ کے لیے SLM بلا معاوضہ فراہم کرتا ہے۔ یہ مواد اُردو کے ذریعے علم حاصل کرنے میں دلچسپی رکھنے والے ہر شخص کے لیے برائے نام قیمت پر دستیاب ہے۔ تعلیم تک رسائی کے دائرے کو مزید پھیلانے کے مقصد سے، اردو/ہندی/انگریزی/عربی میں eSLM یونیورسٹی کی ویب سائٹ پر مفت ڈاؤن لوڈ کے لیے دستیاب رکھا گیا ہے۔

مجھے بے حد خوشی ہے کہ متعلقہ فیکلٹی کی محنت اور مصنفین کے مکمل تعاون کی بدولت FYUG بی۔اے، بی۔ایس سی اور بی۔کام کی کتابوں کی اشاعت کا عمل بڑے پیمانے پر شروع ہو گیا ہے۔ فاصلاتی اور آن لائن لرننگ کے طلبہ کی سہولت کے لیے خود اکتسابی مواد (SLM) کی تیاری اور اشاعت کا عمل یونیورسٹی کے لیے اہمیت رکھتا ہے۔ مجھے یقین ہے کہ ہم اپنے خود تعلیمی مواد کے ذریعے اردو جاننے والے ایک بڑے طبقے کی ضروریات کو پورا کرنے کے قابل ہوں گے اور اس یونیورسٹی کے مقصدِ قیام کو پورا کریں گے اور اپنے ملک میں اپنی موجودگی کو جائز ٹھہرا سکیں گے۔

نیک تمناؤں کے ساتھ!

پروفیسر سید عین الحسن
شیخ الجامعہ، مانو

پیغام

موجودہ دور میں فاصلاتی تعلیم کو دنیا بھر میں ایک نہایت مؤثر اور مفید طریقۂ تعلیم کے طور پر تسلیم کیا جاتا ہے اور بڑی تعداد میں لوگ اس طریقۂ تعلیم سے فائدہ اٹھا رہے ہیں۔ مولانا آزاد نیشنل اردو یونیورسٹی نے بھی اردو زبان بولنے والے عوام کی تعلیمی ضروریات کو مد نظر رکھتے ہوئے اپنے قیام کے وقت سے ہی فاصلاتی تعلیم کا طریقہ متعارف کرایا۔ مولانا آزاد نیشنل اردو یونیورسٹی نے 1998 میں ڈائریکٹوریٹ آف ڈسٹنس ایجوکیشن (نظامتِ فاصلاتی تعلیم) کے ساتھ کام کا آغاز کیا اور 2004 سے باقاعدہ پروگرام شروع ہوئے، اس کے بعد مختلف شعبہ جات قائم کیے گئے۔

یو جی سی نے ملک میں نظام تعلیم کو مؤثر طور پر منظم کرنے میں ایک اہم کردار ادا کیا ہے۔ اوپن اینڈ ڈسٹنس لرننگ (ODL) موڈ کے تحت چلنے والے مختلف پروگرام، جو سینٹر فار ڈسٹنس اینڈ آن لائن ایجوکیشن (CDOE) میں چل رہے ہیں، یو جی سی-ڈی ای بی کے منظور شدہ ہیں۔ یو جی سی-ڈی ای بی نے فاصلاتی اور باقاعدہ تعلیم کے نصاب کو ہم آہنگ کرنے پر زور دیا ہے تاکہ فاصلاتی تعلیم حاصل کرنے والے طلبہ کے معیار کو بہتر بنایا جاسکے۔ چونکہ مولانا آزاد نیشنل اردو یونیورسٹی ایک دُہرے طرز (ڈوئل موڈ) کی یونیورسٹی ہے جو فاصلاتی اور روایتی دونوں طریقۂ تعلیم کی خدمات فراہم کرتی ہے، اس لیے اپنے مقاصد کو یو جی سی-ڈی ای بی کے رہنما خطوط کے مطابق حاصل کرنے کے لیے اس نے چوائس بیسڈ کریڈٹ سسٹم (CBCS) متعارف کرایا گیا جس کا خود اکتسابی مواد (Self Learning Materials) یو جی سی کے قوانین اور کریڈٹ فریم کے مطابق نئے سرے سے تیار کیے جاچکا ہے۔

سینٹر فار ڈسٹنس اینڈ آن لائن ایجوکیشن (CDOE) کل انیس (19) پروگرام پیش کرتا ہے جن میں یو جی، پی جی، بی ایڈ، ڈپلومہ اور سرٹیفکیٹ پروگرام شامل ہیں۔ اس کے ساتھ ساتھ تکنیکی مہارتوں پر مبنی پروگرام بھی شروع کیے جارہے ہیں۔ سی ڈی اوای نے جولائی 2025 سے این ای پی-2020 کے مطابق چار سالہ یو جی پروگرام کا آغاز کیا ہے۔ بی اے، بی ایس سی اور بی کام کے آنرز پروگراموں کو این سی ایف کے مطابق ڈیزائن کیا گیا ہے جس سے طلبہ کو آنرز ڈگری حاصل کرنے میں مدد ملے گی۔ سال 2025-2026 سے ایم بی اے پروگرام او ڈی ایل موڈ میں متعارف کرایا گیا ہے۔

مانو نے طلبہ کی سہولت کے لیے نو ریجنل سنٹرز (بنگلورو، بھوپال، دربھنگہ، دہلی، کولکاتا، ممبئی، پٹنہ، رانچی اور سری نگر) اور چھ سب ریجنل سنٹرز (حیدر آباد، لکھنؤ، جموں، نوح، وارانسی اور امراوتی) کا ایک وسیع نیٹ ورک قائم کیا ہے۔ اس کے علاوہ وجے واڑا میں ایک ایکسٹینشن سنٹر بھی قائم کیا گیا ہے۔ ان ریجنل اور سب ریجنل سنٹروں کے تحت ایک سو پچاس سے زیادہ لرنر سپورٹ سنٹر (LSCs) اور بیس پروگرام سنٹر بیک وقت چلائے جارہے ہیں تاکہ طلبہ کو تعلیمی اور انتظامی سہولیات فراہم کی جاسکیں۔ سینٹر فار ڈسٹنس اینڈ آن لائن ایجوکیشن اپنی تعلیمی اور انتظامی سرگرمیوں میں آئی سی ٹی کا بھرپور استعمال کرتا ہے اور اپنے تمام پروگراموں میں صرف آن لائن موڈ کے ذریعے ہی داخلے فراہم کرتا ہے۔

طلبہ کے لیے سیلف لرننگ میٹیریل (SLM) کی سوفٹ کاپی سینٹر فار ڈسٹنس اینڈ آن لائن ایجوکیشن کی ویب سائٹ پر دستیاب کرائی جاتی ہیں اور آڈیو و ویڈیو ریکارڈنگ کے لنک بھی ویب سائٹ پر فراہم کیے جاتے ہیں۔ اس کے علاوہ طلبہ کو ای۔ میل اور واٹس ایپ گروپ کی سہولت بھی فراہم کی جارہی ہے جن کے ذریعے انہیں پروگرام کے مختلف پہلوؤں جیسے کورس رجسٹریشن، اسائنمنٹ، کاؤنسلنگ، امتحانات وغیرہ کے بارے میں مطلع کیا جاتا ہے۔ باقاعدہ کاؤنسلنگ کے علاوہ گزشتہ دو برسوں سے طلبہ کے تعلیمی معیار کو بہتر بنانے کے لیے زائد تدارکی (Remedial) آن لائن کاؤنسلنگ بھی فراہم کی جارہی ہے۔

امید کی جاتی ہے کہ سینٹر فار ڈسٹنس اینڈ آن لائن ایجوکیشن تعلیمی اور معاشی طور پر پسماندہ آبادی کو عصری تعلیم کے دھارے میں شامل کرنے میں ایک اہم کردار ادا کرے گا۔ تعلیمی ضروریات کو مد نظر رکھتے ہوئے نئی تعلیمی پالیسی (NEP-2020) کے مطابق مختلف پروگرامز میں تبدیلیاں کی گئی ہیں اور توقع ہے کہ اس سے اوپن اینڈ ڈسٹنس لرننگ کے نظام کو مزید مؤثر اور کارآمد بنانے میں مدد ملے گی۔

پروفیسر محمد رضا اللہ خان

ڈائرکٹر، سی ڈی اوای، مانو

کورس کا تعارف

یہ کورس سائبر سیکیورٹی (Cyber Security) کے بنیادی تصورات، خطرات، حملوں اور حفاظتی اقدامات کا تعارف فراہم کرتا ہے۔اس کورس میں طلبہ کو ڈیجیٹل ماحول میں موجود مختلف سیکیورٹی خطرات اور ان سے محفوظ رہنے کے طریقوں سے آگاہ کیا جائے گا۔

کورس کے دوران موبائل اور وائرلیس کمپیوٹنگ، تنظیمی سائبر سیکیورٹی، ڈیٹا پرائیویسی، سائبر کرائم، ویب تھریٹس، سوشل میڈیا سیکیورٹی اور سماجی کمپیوٹنگ جیسے اہم موضوعات کا مطالعہ کیا جائے گا۔

اس کورس میں طلبہ یہ سمجھ سکیں گے کہ سائبر حملے افراد، تنظیموں اور ان کے ڈیٹا کو کس طرح متاثر کر سکتے ہیں۔اس کے ساتھ ساتھ Confidentiality، Integrity اور Availability جیسے بنیادی سیکیورٹی اصولوں، ڈیٹا کے تحفظ، رازداری کی پالیسیوں، رسائی کے کنٹرول اور مختلف حفاظتی اقدامات کا بھی مطالعہ کیا جائے گا۔

کورس کا بنیادی مقصد طلبہ میں سائبر سیکیورٹی کے حوالے سے بنیادی معلومات، سیکیورٹی آگاہی اور محفوظ ڈیجیٹل طریقہ کار کو فروغ دینا ہے، تاکہ وہ مختلف سائبر خطرات کو سمجھ سکیں اور مناسب حفاظتی اقدامات اختیار کر سکیں۔

پروفیسر پردیپ کمار
کورس کوآرڈینیٹر

اکائی 1۔ سائبر سیکیورٹی کا تعارف

(Introduction to Cyber security)

اکائی کے اجزاء

1.0 تمہید

1.1 مقاصد

1.2 سائبر سیکیورٹی(Cyber security)کا تعارف اور اس کی بنیادی باتیں

1.3 سائبر سیکورٹی(Cyber security)کیا ہے؟

1.4 سائبر سیکیورٹی(Cyber security)کیوں ضروری(Importance)ہے؟

1.5 سائبر سیکورٹی(Cyber security)کے بنیادی اصول(Fundamentals)-

1.6 سائبر حملوں(Cyber attack)کی اقسام

1.7 کمزوری، خطرہ، نقصان دہ کام(Vulnerability, threat, Harmful acts)

1.8 کمپیوٹر مجرم(Computer criminal)

1.9 اکتسابی نتائج

1.10 کلیدی الفاظ

1.11 نمونہ امتحانی سوالات

1.12 تجویز کردہ اکتسابی مواد

1.0 تمہید

سائبر سیکیورٹی آج کے ڈیجیٹل دور میں ایک اہم شعبہ ہے۔ سائبر خطرات اور سائبر حملوں میں مسلسل اضافہ ہو رہا ہے اور حملہ آور جدید تکنیکوں کا استعمال کرتے ہوئے کمپیوٹر سسٹمز، نیٹ ورکس اور ڈیٹا کو نشانہ بناتے ہیں۔ افراد، چھوٹے کاروبار اور بڑی تنظیمیں سب سائبر حملوں سے متاثر ہو سکتی ہیں۔ اس لیے سائبر سیکیورٹی کا مقصد سسٹمز، نیٹ ورکس، پروگرامز اور ڈیٹا کو غیر مجاز رسائی، نقصان اور حملوں سے محفوظ رکھنا ہے

1.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- سائبر سیکیورٹی کے بنیادی تصور کو سمجھ سکے گا۔
- سائبر سیکیورٹی کی اہمیت بیان کر سکے گا۔
- سائبر سیکیورٹی کے بنیادی اصول Confidentiality, Integrity اور Availability (CIA Triad) کو سمجھ سکے گا۔
- مختلف سائبر حملوں کی اقسام کی وضاحت کر سکے گا۔
- Vulnerability، Threat اور Attack میں فرق سمجھ سکے گا۔
- کمپیوٹر کرائم اور کمپیوٹر مجرم کے تصور کو سمجھ سکے گا۔
- سائبر سیکیورٹی کی مختلف پرتوں اور حفاظتی اقدامات کو بیان کر سکے گا۔

1.2 سائبر سیکیورٹی (Cyber security) کا تعارف اور اس کی بنیادی باتیں:

سائبر سیکورٹی (Cyber security) سب سے زیادہ فکر مند معاملہ ہے کیونکہ سائبر خطرات (Cyber threats) اور (Attacks) بڑھ رہے ہیں۔ حملہ (Attacks) آور اب سسٹم کو نشانہ بنانے کے لیے مزید جدید ترین (Latest) تکنیکوں کا استعمال کر رہے ہیں۔ افراد (people)، چھوٹے پیمانے پر کاروبار (Business) یا بڑی تنظیم (Organization)، سبھی متاثر ہو رہے ہیں۔ لہذا، یہ تمام فرمیں (Firms) چاہے وہ آئی ٹی (IT) ہوں یا غیر آئی ٹی (Non-IT) فرمس سائبر سیکیورٹی (Cyber security) کی اہمیت کو سمجھ چکی ہیں اور سائبر خطرات (Cyber threats) سے نمٹنے کے لیے تمام ممکنہ اقدامات (Steps) کو اپنانے پر توجہ مرکوز (Focus) کر رہی ہیں۔

1.3 سائبر سیکورٹی (Cyber security) کیا ہے؟

"سائبر سیکورٹی (Cyber security) بنیادی طور پر لوگوں، عملوں اور ٹیکنالوجیز (technology) کے بارے میں ہے جو مل کر کام کر رہے ہیں تاکہ خطرے میں کمی، روک تھام (deterrence)، بین الاقوامی مصروفیت (International engagement)، واقعے کے رد عمل، لچک، اور بحالی کی پالیسیاں اور سرگرمیاں شامل ہوں، بشمول کمپیوٹر نیٹ ورک (computer network) آپریشنز، معلومات کی یقین دہانی، قانون نافذ کرنے والے ادارے وغیرہ۔"

یا

سائبر سیکورٹی ٹیکنالوجیز (cyber security technology)، عمل، اور طریقوں کا باڈی ہے جو نیٹ

ورکس(networks)، کمپیوٹرز، پروگراموں(computer program) اور ڈیٹا کو (Attacks)، نقصان یا غیر مجاز رسائی(Authorized access)سے بچانے کے لیے ڈیزائن کیا گیا ہے۔

سائبر سیکیورٹی(Cyber security)کی اصطلاح سے مراد ڈیجیٹل ڈیٹا(Digital data)کی حفاظت کے لیے تیار کی گئی تکنیکوں(techniques)اور طریقوں سے ہے۔

وہ ڈیٹا جو انفارمیشن سسٹم(information system)میں محفوظ، منتقل یا استعمال ہوتا ہے۔

یا

سائبر سیکیورٹی(Cyber security) انٹرنیٹ سے منسلک سسٹمز کا تحفظ(protection) ہے، بشمول (including)ہارڈویئر(hardware)، سافٹ ویئر(software)، اور سائبر حملوں(cyber threats)سے ڈیٹا۔

یہ دو الفاظ سے بنا ہے ایک سائبر(cyber)اور دوسرا سیکورٹی(Security)۔

سائبر کا تعلق اس ٹیکنالوجی سے ہے جس میں سسٹم، نیٹ ورک(system network)اور پروگرام یا ڈیٹا(program data)ہوتا ہے۔ جبکہ تحفظ سے متعلق سیکورٹی(security) جس می سسٹم سیکورٹی(system security)، نیٹ ورک سیکورٹی(network security)، ایپلیکیشن(application) اور انفارمیشن سیکورٹی(information security) شامل ہے۔

1.4 سائبر سیکیورٹی(Cyber security) کیوں ضروری(importance) ہے؟

ذیل میں درج وضوہات ہیں جن کی وجہ سے ڈیجیٹل دنیا(digital world)میں سائبر سیکیورٹی(Cyber security) اتنی اہم ہے:

کاروباری اداروں کے لیے(cyber attacks)بہت مہنگے ہو سکتے ہیں۔

کاروبار کو پہنچنے والے مالی نقصان کے علاوہ، ڈیٹا(data)کی خلاف ورزی سے نام نہاد ساکھ کو نقصان بھی پہنچ سکتا ہے۔

سائبر(cyber attacks)ان دنوں بتدریج تباہ کن(Gradually destructive)ہوتے جا رہے ہیں۔ سائبر جرائم پیشہ افراد(Cyber criminals)سائبر حملوں(cyber attacks)کو شروع کرنے کے لیے زیادہ نفیس طریقے استعمال کر رہے ہیں۔

جی ڈی پی آر(GDPR)جیسے ضوابط تنظیموں(Regulations organizations)کو اپنے پاس رکھے ہوئے ذاتی ڈیٹا کی بہتر دیکھ بھال کرنے پر مجبور کر رہے ہیں۔

مندرجہ بالا وضوہات کی بنا پر، سائبر سیکیورٹی(Cyber security)کاروبار کا ایک اہم حصہ بن گیا ہے اور اب توجہ مناسب رد عمل کے منصوبے تیار کرنے پر ہے جو سائبر(Attacks)کی صورت میں نقصان کو کم سے کم کریں۔

لیکن، ایک تنظیم یا فرد صرف اس وقت مناسب جوابی منصوبہ تیار کر سکتا ہے جب سائبر سیکیورٹی(Cyber security) کے بنیادی اصولوں پر اس کی اچھی گرفت ہو۔

1.5 سائبر سیکورٹی(Cyber security) کے بنیادی اصول(Fundamentals)

رازداری(Confidentiality)

رازداری(Confidentiality) غیر مجاز جماعتوں(unauthorized parties) کو ڈیٹا(data) کے افشاء کو روکنے کے بارے میں ہے۔

اس کا مطلب یہ بھی ہے کہ ڈیٹا (data) کو شیئر(share) کرنے اور رکھنے میں ملوث مجاز فریقوں(authorized parties) کی شناخت کو نجی(Private) اور گمنام(anonymous) رکھنے کی کوشش کرتا ہے۔

ناقص خفیہ کردہ ڈیٹا(Poorly encrypted data) کو کریک(crack) کرنے، مین-ان-دی-مڈل(MITM Attacks)، حساس ڈیٹا(Sensitive data) کو ظاہر کرنے سے اکثر رازداری سے سمجھوتہ کیا جاتا ہے۔

رازداری قائم کرنے کے معیاری اقدامات(Standard measures) میں شامل ہیں:

ڈیٹا کی خفیہ کاری(Data encryption)

- دو عنصر کی توثیق(Two-factor authentication)
- بائیومیٹرک تصدیق(Biometric authentication)
- سیکیورٹی ٹوکنز(Security tokens)

سالمیت(Integrity)

- سالمیت(Integrity) سے مراد غیر مجاز فریقوں(Parties) کے ذریعہ معلومات کو تبدیل کرنے سے بچانا ہے۔

سالمیت(Integrity) کی ضمانت کے معیاری اقدامات میں شامل ہیں:

- کرپٹو گرافک چیکسم(Cryptographic checksum)
- فائل کی اجازتوں کا استعمال(Using file permissions)
- بلا تعطل بجلی کی فراہمی(Uninterrupted power supply)
- ڈیٹا بیک اپ(Data Backup)
- دستیابی(Availability)
- دستیابی(Availability) اس بات کو یقینی بنا رہی ہے کہ مجاز فریقین(authorized Parties) ضرورت پڑنے پر معلومات تک رسائی حاصل کر سکیں۔

دستیابی(Availability)کی ضمانت کے لیے معیاری اقدامات(standard measures)میں شامل ہیں:

- بیرونی ڈرائیوز میں ڈیٹا کا بیک اپ لینا(Backing up data to external drives)
- فائروالز کو نافذ کرنا(Implementing firewalls)
- بیک اپ پاور سپلائیز ہونا(Having backup power supplies)
- ڈیٹا فالتو پن(Data redundancy)

1.6 سائبر حملوں(Cyber attack)کی اقسام

سائبر حملہ(Cyber attacks)کمپیوٹر سسٹمز(Computer systems)اور نیٹ ورکس(networks)کا استحصال ہے۔ یہ کمپیوٹر کوڈ(computer code)، منطق یا ڈیٹا کو تبدیل کرنے کے لیے بدنیتی پر مبنی کوڈ کا استعمال کرتا ہے اور سائبر کرائمز(cyber crimes)، جیسے معلومات اور شناخت کی چوری(Identity theft)کا باعث بنتا ہے۔

سائبر حملوں(Cyber attacks)کو درج ذیل زمروں(categories)میں تقسیم کیا جاسکتا ہے۔

- ویب پر مبنی(Web-based attacks)
- سسٹم پر مبنی(Attacks)ویب پر مبنی(System-based attack)
- ویب پر مبنی(Web-based attacks)

یہ وہ(Attacks)ہیں جو کسی ویب سائٹ(website)یا ویب ایپلیکیشنز(webapplication)پر ہوتے ہیں۔ ویب پر مبنی کچھ اہم(Attacks)درج ذیل ہیں۔

1۔ **انجیکشن(Injection)کے(Attacks):** یہ وہ حملہ(attack)ہے جس میں ایپلی کیشن(application)میں ہیرا پھیری کرنے اور مطلوبہ معلومات حاصل کرنے کے لیے کچھ ڈیٹا(data)کو ویب ایپلیکیشن(web application)میں داخل کیا جائے گا:۔ مثال- ایس کیو ایل انجیکشن(SQL Injection)، کوڈ انجیکشن(code injection)، لاگ انجیکشن(log injection)، ایکس ایم ایل انجیکشن(XML Injection)وغیرہ۔

2۔ **DNS سپوفنگ:-** DNS سپوفنگ کمپیوٹر سیکیورٹی ہیکنگ(computer security hacking)کی ایک قسم ہے۔ جس کے ذریعے ڈی این ایس(DNS)حل کرنے والے کیشے(cache)میں ڈیٹا متعارف کرایا جاتا ہے جس کی وجہ سے نام کا سرور غلط IP ایڈریس واپس کرتا ہے، ٹریفک(traffic)کو حملہ(attack)آور کمپیوٹر یا کسی دوسرے کمپیوٹر کی طرف موڑ دیتا ہے۔ DNS سپوفنگ(Attacks)بغیر پتہ چلائے طویل عرصے تک جاری رہ سکتے ہیں اور سیکیورٹی کے سنگین مسائل پیدا کر سکتے ہیں۔

3۔ **سیشن ہائی جیکنگ(Session Hijacking):-** یہ ایک محفوظ نیٹ ورک(secure network)پر صارف(user)کے سیشن(session)پر سیکیورٹی حملہ(security attack)ہے۔ ویب ایپلیکیشنز(web application)ریاست اور

صارف(user) کے سیشنز(sessions) کو ذخیرہ (storage)کرنے کے لیے کوکیز(cookies) بناتی ہیں۔ کوکیز چوری(cookies-theft) کرنے سے، حملہ(attack)آور صارف(user) کے تمام ڈیٹاتک رسائی(access)حاصل کر سکتا ہے۔

4۔ **فشنگ(Phishing):-** فشنگ (Phishing)ایک قسم کا حملہ (attack)ہے جو صارف (user)کے لاگ ان کی اسناد(credentials) اور کریڈٹ کارڈ نمبر (Credit card number)جیسی حساس معلومات (sensitive information)کو چرانے(theft) کی کوشش کرتا ہے۔ یہ اس وقت ہوتا ہے جب کوئی حملہ(attack)آور الیکٹرانک کمیونیکیشن(electronic communication)میں ایک قابل اعتماد ہستی کے طور پر نقاب پوش ہوتا ہے۔

5۔ **وحشیانہ طاقت(Brute force):-** یہ ایک قسم کا حملہ ہے جو آزمائشی (trial)اور غلطی کا طریقہ استعمال کرتا ہے۔ یہ حملہ (attack)بڑی تعداد میں اندازے پیدا کرتا ہے اور صارف(user)کا پاس ورڈ اور ذاتی شناختی نمبر جیسے حقیقی ڈیٹا(real data) حاصل کرنے کے لیے ان کی توثیق(verification) کرتا ہے۔ یہ حملہ مجرموں(Attack criminals)کے ذریعے خفیہ کردہ ڈیٹا(encrypted data) کو کریک(crack) کرنے کے لیے، یا سیکیورٹی (security)کے ذریعے، تجزیہ کار (analyst)کسی تنظیم(organisaion)کے نیٹ ورک سیکیورٹی(network security)کو جانچنے(check)کے لیے استعمال کر سکتے ہیں۔

6۔ **سروس سے انکار(Denial of service):-** یہ ایک حملہ (attack)ہے جس کا مقصد سرور (Server)یا نیٹ ورک(network)کے وسائل کو صارفین(user)کے لیے دستیاب(available) نہیں کرنا تھا۔ یہ ہدف کو ٹریفک سے بھر کر یا اسے ایسی معلومات بھیج کر پورا کرتا ہے جو حادثے کو متحرک کرتی ہے۔ یہ سرور پر حملہ کرنے کے لیے سنگل سسٹم اور سنگل انٹرنیٹ کنیکشن کا استعمال کرتا ہے۔ اسے درج ذیل میں تقسیم کیا جا سکتا ہے۔

- **حجم پر مبنی حملہ(Volume-based attacks):-** اس کا مقصد حملہ شدہ سائٹ(Attacked site)کی بینڈوڈتھ (Bandwidth)کو سیر (share)کرتا ہے، اور اسے بٹ فی سیکنڈ(Bit per second)میں ماپا جاتا ہے۔ پروٹوکول (Protocol attacks)- یہ سرور(server)کے اصل وسائل(Original resources)استعمال کرتا ہے، اور اسے پیکٹ(packet)میں ماپا جاتا ہے۔
- **ایپلیکیشن پرت کے حملہ (Application layer attacks):-** اس کا مقصد ویب سرور(web server)کو کریش(crash) کرنا ہے اور اسے فی سیکنڈ(per second)کی درخواست میں ماپا جاتا ہے۔

7۔ **لغت کے حمل(Attacks Dictionary):-** اس قسم کا حملہ(attack) عام طور پر استعمال ہونے والے پاس ورڈ کی فہرست(password list) کو محفوظ کرتا ہے اور اصل پاس ورڈ (password)حاصل کرنے کے لیے ان کی توثیق(Verification)کرتا ہے۔

8۔ **یو آر ایل کی تشریح(URL interpretation):-** یہ ایک قسم کا حملہ(attack) ہے جہاں ہم یو آر ایل(URL) کے کچھ حصوں کو تبدیل کر سکتے ہیں،اور کوئی ویب سرور(web server) بنا کر ایسے ویب صفحات(Web pages) فراہم کر سکتا ہے جس کے لیے اسے براؤز(Browse) کرنے کا اختیار نہیں ہے۔

9۔ **فائل انکلوژن حمل(File inclusion Attacks):-** یہ ایک قسم کا حملہ(attack) ہے جو حملہ(attack) آور کو غیر مجاز یا ضروری فائلوں تک رسائی حاصل کرنے کی اجازت دیتا ہے جو ویب سرور(web server) پر دستیاب ہے یا شامل فعالیت(functionality) کا استعمال کر کے ویب سرور(web server) پر مبنی فائلوں کو انجام دے سکتا ہے۔

10۔ درمیانی حملوں میں آدمی حمل(Man in the middle attacks):- یہ ایک قسم کا حملہ (attack) ہے جو حملہ آور(attacker) کو کلائنٹ(client) اور سرور(server) کے درمیان رابطے کو روکنے اور ان کے درمیان ایک پل کا کام کرنے دیتا ہے۔اس کی وجہ سے، حملہ(attack) آور روکے گئے کنکشن میں ڈیٹا کو پڑھ، داخل اور اس میں ترمیم(edit) کر سکے گا۔

سسٹم پر مبنی حمل(System-based Attacks)

یہ وہ(Attacks) ہیں جن کا مقصد کمپیوٹر یا کمپیوٹر نیٹ ورک سے سمجھوتہ کرنا ہے۔نظام پر مبنی کچھ اہم(Attacks) درج ذیل ہیں۔

a) وائرس(Virus): یہ ایک قسم کا بدنیتی پر مبنی سافٹ ویئر پروگرام(Software program) ہے جو کسی صارف کے علم کے بغیر کمپیوٹر کی تمام فائلوں میں پھیل جاتا ہے۔ یہ ایک خود ساختہ بدنیتی(Self-inflicted malice) پر مبنی کمپیوٹر پروگرام (computer program) ہے جو اپنے آپ کو دوسرے کمپیوٹر پروگراموں میں ڈال کر نقل کرتا ہے۔ یہ نظام کو نقصان پہنچانے والی ہدایات پر بھی عمل درآمد کر سکتا ہے۔

b) Worm: یہ میلویئر(Malware) کی ایک قسم ہے جس کا بنیادی کام خود کو غیر متاثرہ کمپیوٹرز میں پھیلانے کے لیے نقل کرتا ہے۔ یہ کمپیوٹر وائرس(computer virus) کی طرح کام کرتا ہے۔ کیڑے اکثر ای میل(Email) منسلکات سے پیدا ہوتے ہیں جو بظاہر قابل اعتماد بھیجنے والوں کی طرف سے ہوتے ہیں۔

c) Trojan horse: یہ ایک بدنیتی(Malice) پر مبنی پروگرام(program) ہے جو کمپیوٹر کی ترتیب اور غیر معمولی سرگرمی میں غیر متوقع تبدیلیاں کرتا ہے، یہاں تک کہ جب کمپیوٹر بیکار ہو۔ یہ صارف(user) کو اس کے حقیقی ارادے سے گمراہ کرتا ہے۔بظاہر یہ ایک عام ایپلی کیشن(Application) ہے لیکن جب اسے کھولا یا عمل میں لایا جائے گا تو کچھ بدنیتی پر مبنی کوڈ پس منظر میں چلے گا۔

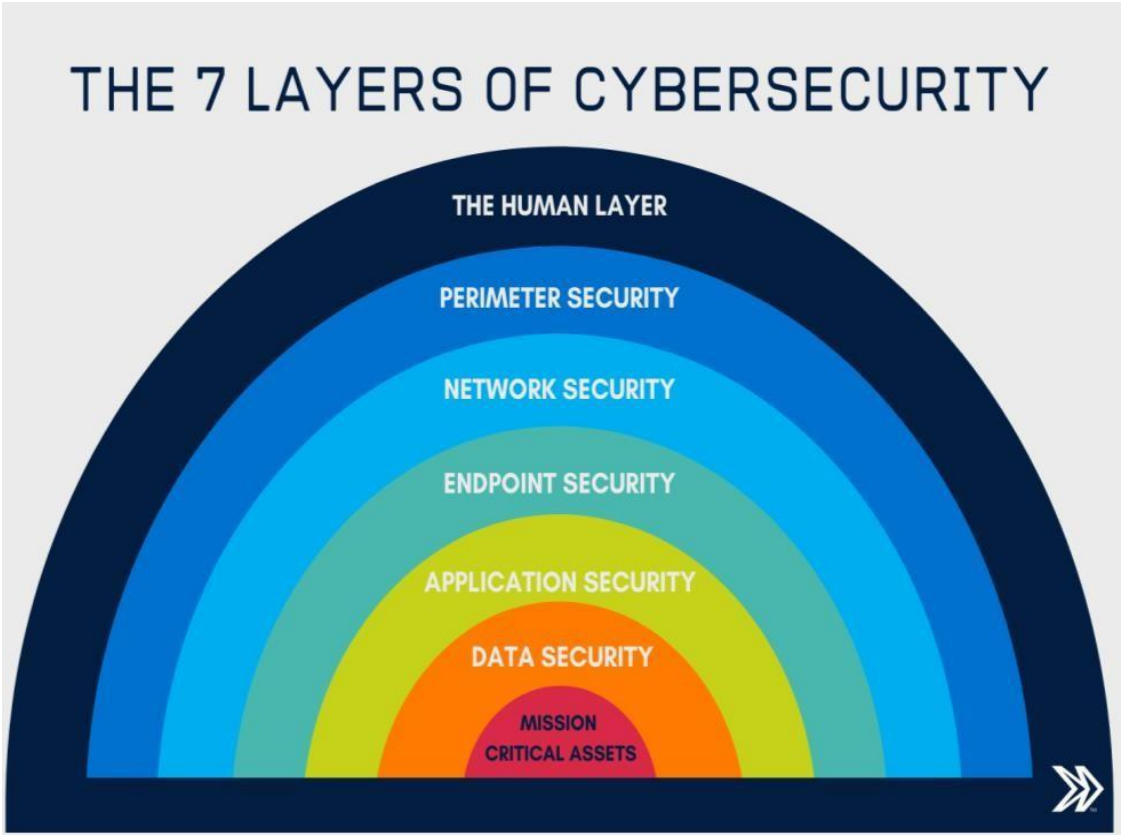
d) Backdoors: یہ ایک ایسا طریقہ ہے جو عام تصدیق کے عمل کو نظرانداز کرتا ہے۔ایک ڈویلپر بیک ڈور بنا(Developer backdoor) سکتا ہے تاکہ کسی ایپلیکیشن(application) یا آپریٹنگ سسٹم (operating system) تک ٹربل شوٹنگ(Troubleshooting) یا دیگر مقاصد کے لیے رسائی حاصل کی جا سکے۔

بوٹس(Bots) A Bot("روبوٹ"[short for robot]) کے لیے مختصر) ایک خودکار عمل ہے جو نیٹ ورک کی دیگر

خدمات کے ساتھ تعامل کرتا ہے۔ کچھ بوٹس پروگرام(Bots program)خود بخود چلتے ہیں، جبکہ دوسرے صرف اس وقت کمانڈز پر عمل درآمد کرتے ہیں جب وہ مخصوص ان پٹ وصول کرتے ہیں۔ بوٹس پروگرام(Bots program) کی عام مثالیں کرالر(Crawler)،چیٹ روم بوٹس(Chat room Bot)،اور بدنیتی پر مبنی بوٹس(Malicious Bot)ہیں۔

سائبر سیکیورٹی(Cyber security) کی 7 پرتیں اس مشن کے اہم اثاثوں پر مرکوز ہونی چاہئیں جن کی آپ حفاظت کرنا چاہتے ہیں۔

مشن کریٹیکل اثاثے(mission critical Assets)- یہ وہ ڈیٹا ہے جس کی آپ کو حفاظت کرنے کی ضرورت ہے۔



ڈیٹا سیکیورٹی(Data security)- ڈیٹا سیکیورٹی کنٹرول(Data security control)ڈیٹا کی اسٹوریج اور منتقلی کی حفاظت کرتے ہیں۔

ایپلیکیشن سیکیورٹی(Application security)- ایپلیکیشنز سیکیورٹی(Application security)کنٹرولز کسی ایپلیکیشن تک رسائی، آپ کے مشن کے اہم اثاثوں تک ایپلیکیشن(application) کی رسائی، اور ایپلیکیشن کی اندرونی سیکیورٹی(security) کی حفاظت کرتے ہیں۔

اینڈ پوائنٹ سیکیورٹی(Endpoint security)- اینڈ پوائنٹ سیکیورٹی(Endpoint security)کنٹرول ڈیوائسز اور کے درمیان کنکشن کی حفاظت کرتے ہیں نیٹ ورک(network) میں۔

نیٹ ورک سیکیورٹی(Network security)-نیٹ ورک سیکیورٹی کنٹرولز(Network security) control تنظیم کے نیٹ ورک کی حفاظت کرتے ہیں اور نیٹ ورک(Network)تک غیر مجاز رسائی کو روکتے ہیں۔

پیری میٹر سیکیورٹی(Parameter security)- پیریمیٹر سیکیورٹی کنٹرولز(Parameter security)میں جسمانی اور ڈیجیٹل سیکیورٹی(Digital security)دونوں طریقے شامل ہیں جو کاروبار کو مجموعی طور پر تحفظ فراہم کرتے ہیں۔

انسانی پرت(Human layer)-انسان کسی بھی سائبر سیکورٹی(cyber security) پوزیشن میں سب سے کمزور کڑی ہیں۔ ہیومن سیکیورٹی کنٹرولز(Human security controls)میں فشنگ سمیولیشنز(phshing simulations)اور رسائی کے انتظام کے کنٹرول شامل ہیں جو مشن کے اہم اثاثوں کو مختلف قسم کے انسانی خطرات سے بچاتے ہیں، بشمول سائبر(Cyber Inclusion)مجرم، بدنیتی(Malice)پر مبنی اندرونی، اور لاپرواہ صارفین۔

1.7 کمزوری، خطرہ، نقصان دہ کام(Vulnerability, threat, Harmful acts)

Cyber Threat: سائبر خطرات سیکیورٹی(Cyber threat security)کے واقعات(incident)یا حالات ہیں جن کے منفی(negative)ہونے کے امکانات ہیں۔ آپ کے نیٹ ورک یا دیگر ڈیٹا مینجمنٹ سسٹمز کا(other data management system)نتیجہ۔ سیکیورٹی خطرات(security attacks)کی عام اقسام کی مثالوں میں فشنگ حملے(phising attack)شامل ہیں جن کے نتیجے میں میلویئر(malware)کی تنصیب جو آپ کے ڈیٹا کو متاثر کرتی ہے، عملے کے رکن کی ڈیٹا کی پیروی کرنے میں ناکامی۔ حفاظتی پروٹوکول(protection protocol) جو ڈیٹا کی خلاف ورزی کا سبب بنتے ہیں، یا یہاں تک کہ ایک طوفان(tornado)جو آپ کو نیچے لے جاتا ہے۔ کمپنی کا ڈیٹا ہیڈ کوارٹر(head quarter)، رسائی میں خلل ڈال رہا ہے۔

کمزوریاں(Vulnerabilities): کمزوریاں(Vulnerabilities)ایسے نظام میں موجود خلاء یا کمزوریاں ہیں جو خطرات کو ممکن اور آزمائش بناتی ہیں۔ نیٹ ورک سیکورٹی میں کمزوریوں(Vulnerabilities) کی اقسام میں SQL انجیکشن (SQL Injection)شامل ہیں لیکن ان تک محدود نہیں ہیں، سرور کی غلط کنفیگریشنز(server misconfiguaration)، کراس سائٹ(cross site)اسکرپٹنگ(scripting)، اور حساس ڈیٹا کو غیر خفیہ کردہ سادہ ٹیکسٹ فارمیٹ میں منتقل کرنا۔

جب خطرے(attack)کے امکان کو ممکنہ نقصان سے ضرب دیا جاتا ہے جس کے نتیجے میں ہو سکتا ہے، سائبر سیکیورٹی ماہرین، اسے ایک خطرہ کے طور پر حوالہ دیتے ہیں۔

سیکورٹی کے خطرات، دھمکیاں اور حملے(Security Vulnerabilities, Threats and Attacks)

کمزوریوں کے زمرے(categories)

- لیکی(Leaky)(رازداری(confidentiality)کا نقصان)
- خراب(corrupted)(سالمیت(Integrity)کا نقصان)

- غیر دستیاب(Unavailable)یا بہت سست(slow)(دستیابیت(availability)کا نقصان)
- جب خطرات سے فائدہ اٹھایا جاتا ہے تو خطرات کسی اثاثہ کو ممکنہ حفاظتی نقصان کی نمائندگی کرتے ہیں۔

(Attacks)وہ دھمکیاں ہیں جو کئے گئے ہیں۔

- غیر فعال(Passive)- سسٹم کے وسائل کو متاثر کیے بغیر سسٹم سے معلومات کا استعمال کریں۔
- فعال(Active)- سسٹم کے وسائل کو تبدیل کریں یا آپریشن کو متاثر کریں۔
- اندرونی(Insider)- تنظیم کے اندر ایک ہستی کے ذریعہ شروع کیا گیا ہے۔
- بیرونی(Outsider)-دائرہ کے باہر سے شروع کیا گیا۔

1.8 کمپیوٹر مجرم(Computer criminal)

کمپیوٹر مجرموں(Computer criminal)کو ہارڈ ویئر(hardware)، سافٹ ویئر(software)اور ڈیٹا کی بہت زیادہ مقدار تک رسائی حاصل ہے۔ان کے پاس پوری دنیا میں موثر کاروبار اور حکومت کو تباہ کرنے کی صلاحیت ہے۔ایک لحاظ سے، کمپیوٹر سیکیورٹی(computer security)کا مقصد ان مجرموں(Criminals)کو نقصان پہنچانے سے روکنا ہے۔

ہم کہتے ہیں۔ کمپیوٹر جرم(computer crime)کوئی بھی جرم(crime)ہے جس میں کمپیوٹر شامل ہے یا اس کے استعمال سے مدد ملتی ہے۔اگرچہ یہ تعریف بہت وسیع ہے، لیکن یہ ہمیں اپنے آپ کو،اپنے کاروباروں،اور اپنی برادریوں کو ان لوگوں کے خلاف محفوظ رکھنے کے طریقوں پر غور کرنے کی اجازت دیتی ہے جو کمپیوٹر کو بدنیتی(Malice)سے استعمال کرتے ہیں۔

روک تھام یا اعتدال کا ایک طریقہ یہ سمجھنا ہے کہ یہ جرائم(crime)کون کرتا ہے اور کیوں کرتا ہے۔ بہت سے مطالعات نے کمپیوٹر مجرموں(crimes)کی خصوصیات کا تعین کرنے کی کوشش کی ہے۔ان لوگوں کا مطالعہ کرنے سے جنہوں نے پہلے ہی جرائم (crime)کے ارتکاب کے لیے کمپیوٹر کا استعمال کیا ہے، ہم مستقبل میں ممکنہ مجرموں کو تلاش کرنے اور جرائم کو ہونے سے روکنے کے قابل ہو سکتے ہیں۔

سی آئی اے ٹرائیڈ(CIA Traid)

CIA Triad دراصل ایک سیکورٹی ماڈل(security model)ہے جو لوگوں کو IT سیکورٹی کے مختلف حصوں کے بارے میں سوچنے میں مدد کرنے کے لیے تیار کیا گیا ہے۔

سی آئی اے(CIA)کی تین شاخیں ٹوٹ گئیں:

رازداری(Confidential)

آج کی دنیا میں لوگوں کے لیے اپنی حساس، نجی(private)معلومات کو غیر مجاز رسائی(Unauthorized access) سے بچانا بہت ضروری ہے۔رازداری(privacy)کی حفاظت کا انحصار اس بات پر ہے کہ وہ معلومات تک رسائی کی مخصوص سطحوں کو

متعین اور نافذ کر سکے۔ کچھ معاملات میں، ایسا کرنے میں معلومات کو مختلف مجموعوں میں الگ کرنا شامل ہوتا ہے جو کہ کس کے ذریعہ ترتیب دیا جاتا ہے کہ کس کو معلومات تک رسائی کی ضرورت ہے اور وہ معلومات در حقیقت کتنی حساس ہے۔یعنی رازداری کی خلاف ورزی کی صورت میں ہونے والے نقصان کی مقدار۔

رازداری(privacy)کا انتظام کرنے کے لیے استعمال ہونے والے کچھ سب سے عام ذرائع میں رسائی کنٹرول فہرستیں، حجم اور فائل کی خفیہ کاری، اور یونکس فائل کی اجازتیں شامل ہیں۔

سالمیت(Integrity):-ڈیٹا انٹیگریٹی(Data integrity)وہی ہے جس کا مطلب CIA Triad میں "I" ہے۔

یہ CIA Triad کا ایک لازمی جزو ہے اور کسی بھی غیر مجاز فریق سے ڈیٹا کو حذف یا ترمیم سے بچانے کے لیے ڈیزائن کیا گیا ہے، اور یہ اس بات کو یقینی بناتا ہے کہ جب کوئی بااختیار شخص کوئی ایسی تبدیلی کرتا ہے جسے نہیں ہونا چاہیے تھا تو نقصان کو واپس کیا جا سکتا ہے۔

دستیابی(Availability):-یہ CIA Triad کا حتمی جزو ہے اور اس سے مراد آپ کے ڈیٹا کی اصل دستیابی (Availability)ہے۔ تصدیق کے طریقہ کار، رسائی کے چینلز اور سسٹمز کو ان معلومات کے لیے مناسب طریقے سے کام کرنا ہوگا جس کی وہ حفاظت کرتے ہیں اور اس بات کو یقینی بناتے ہیں کہ جب اس کی ضرورت ہو دستیاب(Availability)ہو۔

سی آئی اے (CIA)ٹرائیڈ کو سمجھنا:-سی آئی اے (CIA)ٹرائیڈ تمام معلومات کے بارے میں ہے۔ اگرچہ یہ آئی ٹی سیکورٹی(security)کی اکثریت کا بنیادی عنصر سمجھا جاتا ہے، یہ سیکورٹی(security)کے محدود نقطہ نظر کو فروغ دیتا ہے جو دیگر اہم عوامل کو نظرانداز کرتا ہے.

مثال کے طور پر، اگرچہ دستیابی(availability)اس بات کو یقینی بنانے کے لیے کام کر سکتی ہے کہ آپ معلومات فراہم کرنے کے لیے درکار وسائل تک رسائی سے محروم نہ ہوں جب اس کی ضرورت ہو، خود معلومات کے تحفظ کے بارے میں سوچنا اس بات کی ضمانت نہیں دیتا کہ کسی اور نے آپ کے ہارڈ ویئر(hardware)کے وسائل کو اجازت کے بغیر استعمال نہیں کیا ہے۔.

یہ سمجھنا ضروری ہے کہ CIA Triad کیا ہے، اسے منصوبہ بندی کے لیے کیسے استعمال کیا جاتا ہے اور اس کے پیچھے موجود مختلف اصولوں کو سمجھتے ہوئے ایک معیاری سیکیورٹی پالیسی(security policy)پر عمل درآمد(import) بھی کیا جاتا ہے۔ اس کی پیش کردہ حدود(limitation)کو سمجھنا بھی ضروری ہے۔ جب آپ کو مطلع کیا جاتا ہے، تو آپ سی آئی اے ٹرائیڈ(CIA Traid)کو اس کے لیے استعمال کر سکتے ہیں جو اسے پیش کرنا ہے اور ان نتائج(result)سے بچ سکتے ہیں جو اسے نہ سمجھ کر سامنے آ سکتے ہیں۔

1.9 اکتسابی نتائج

- سائبر سیکیورٹی کی تعریف کر سکے گا۔
- سائبر سیکیورٹی کی ضرورت اور اہمیت بیان کر سکے گا۔
- CIA Triad یعنی Confidentiality ، Integrity اور Availability کی وضاحت کر سکے گا۔

- مختلف سائبر حملوں جیسے Phishing, SQL Injection, DNS Spoofing, Session Hijacking, Brute Force, DoS, Virus, Worm اور Trojan Horse کو پہچان سکے گا۔
- Vulnerability، Threat اور Attack کے درمیان فرق واضح کر سکے گا۔
- سائبر مجرم اور کمپیوٹر کرائم کے بنیادی تصورات سمجھ سکے گا۔

1.10 کلیدی الفاظ

- Cyber Security
- Cyber Threat
- Cyber Attack
- Confidentiality
- Integrity
- Availability
- CIA Triad
- Vulnerability
- Phishing
- SQL Injection
- DNS Spoofing
- Session Hijacking
- Brute Force
- Denial of Service (DoS)
- Virus
- Worm
- Trojan Horse
- Backdoor
- Bot
- Computer Crime

- Computer Criminal
- Network Security
- Data Security
- Application Security
- Endpoint Security

1.11 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات

1۔ سائبر سیکیورٹی سے کیا مراد ہے؟

2۔ رازداری (Confidentiality) کیا ہے؟

3۔ سائبر خطرہ (Cyber Threat) کیا ہے؟

4۔ فِشنگ (Phishing) کیا ہے؟

5۔ کمپیوٹر جرم (Computer Crime) کیا ہے؟

مختصر جوابات کے حامل سوالات

1۔ سائبر سیکیورٹی کی اہمیت بیان کریں۔

2۔ سائبر سیکیورٹی کے تین بنیادی اصول (CIA Triad) کی وضاحت کریں۔

3۔ ویب پر مبنی سائبر حملوں کی مختلف اقسام بیان کریں۔

4۔ انجیکشن اٹیک، DNS Spoofing اور Session Hijacking کی وضاحت کریں۔

5۔ فِشنگ، Brute Force اور Denial of Service (DoS) حملوں کی وضاحت کریں۔

6۔ سسٹم پر مبنی حملوں کی مختلف اقسام مثالوں کے ساتھ بیان کریں۔

7۔ Vulnerability، Threat اور Attack کی وضاحت کریں۔

8۔ سائبر سیکیورٹی کی مختلف پرتوں (Layers) کی وضاحت کریں۔

طویل جوابات کے حامل سوالات

1۔ سائبر سیکیورٹی کی تعریف بیان کرتے ہوئے اس کی اہمیت، بنیادی اصولوں اور حفاظتی اقدامات کی تفصیل سے وضاحت کریں۔

2۔ مختلف سائبر حملوں کی اقسام بیان کریں۔ ویب پر مبنی اور سسٹم پر مبنی حملوں کی تفصیل مثالوں کے ساتھ بیان کریں۔

3۔ CIA Triad کی تفصیل سے وضاحت کریں۔ رازداری (Confidentiality)، سالمیت (Integrity) اور دستیابی (Availability) کو مناسب مثالوں اور حفاظتی اقدامات کے ساتھ بیان کریں۔

1.12 تجویز کردہ اکتسابی مواد

1۔ Cyber Security کا تعارف اور بنیادی تصورات

2۔ Cyber Security کی اہمیت

3۔ CIA Triad

4۔ Cyber Attacks کی اقسام

5۔ Web-based اور System-based Attacks

6۔ Vulnerability, Threat اور Attack

7۔ Computer Crime اور Computer Criminal

اکائی 2۔ سائبر حملے اور سیکیورٹی پالیسیاں

(Cyber Security and Security Policies)

اکائی کے اجزاء

2.0 تمہید

2.1 مقاصد

2.2 اثاثے اور خطرہ (Assets and risk)

2.3 حملہ آوروں کے محرکات (Motives of the attackers)

2.4 حملہ کے اقسام (Types of attacks)

2.5 ہارڈویئر حملوں (Hardware attacks)

2.6 سیکورٹی پالیسیاں (Security policies)

2.7 اکتسابی نتائج

2.8 کلیدی الفاظ

2.9 نمونہ امتحانی سوالات

2.10 تجویز کردہ اکتسابی مواد

2.0 تمہید

اس اکائی میں سائبر سیکیورٹی سے متعلق اثاثے (Assets) ، خطرات (Threats) ، حملہ آوروں کے محرکات (Motives)، سائبر حملوں کی اقسام، ہارڈویئر حملے اور سیکیورٹی پالیسیاں شامل ہیں۔ اس اکائی کے ذریعے طلبہ یہ سمجھتے ہیں کہ کسی تنظیم کے اہم اثاثے کون سے ہیں، انہیں کن خطرات کا سامنا ہو سکتا ہے، حملہ آور سائبر حملے کیوں کرتے ہیں اور مختلف حملوں سے بچاؤ کے لیے سیکیورٹی پالیسیوں کا کیا کردار ہے۔

2.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- اثاثے (Assets) اور خطرات (Threats) کے بنیادی تصورات کو سمجھ سکے گا۔
- سائبر حملہ آوروں کے مختلف محرکات (Motives) کی وضاحت کر سکے گا۔
- سائبر حملوں کی مختلف اقسام کو سمجھ سکے گا۔
- Activeاور Passive Attacks میں فرق کر سکے گا۔
- مختلف Softwareاور Hardware Attacks کی وضاحت کر سکے گا۔
- Cyber Warfare،Cyber Crime، Cyber Terrorismاور Cyber Espionage کو سمجھ سکے گا۔
- Security Policies کی اہمیت اور مختلف اقسام کی وضاحت کر سکے گا۔

2.2 اثاثے اور خطرہ (Assets and Threat)

اثاثہ (Assets) کیا ہے: ایک اثاثہ (Assets) کسی تنظیم کے سسٹمز (systems) کا کوئی بھی ڈیٹا، ڈیوائس (device) یا دیگر جز ہوتا ہے جو کہ قیمتی ہوتا ہے—اکثر اس لیے کہ اس میں حساس ڈیٹا ہوتا ہے یا ایسی معلومات تک رسائی کے لیے استعمال کیا جا سکتا ہے۔

مثال کے طور پر: کسی ملازم کے ڈیسک ٹاپ (desktop) کمپیوٹر (computer)، لیپ ٹاپ (laptop) یا کمپنی کے فون کو ایک اثاثہ (assets) سمجھا جائے گا، جیسا کہ ان آلات پر ایپلی کیشنز (appli cations) ہوں گی۔ اسی طرح، اہم انفراسٹرکچر (infrastructure)، جیسے سرورز (server) اور سپورٹ سسٹم (support system)، اثاثے (asset) ہیں۔ ایک تنظیم کے سب سے عام اثاثے (asset) معلوماتی اثاثے ہیں۔ یہ چیزیں ہیں جیسے ڈیٹا بیس اور فزیکل فائلز (phyicals)- یعنی وہ حساس ڈیٹا جسے آپ اسٹور کرتے ہیں۔

خطرہ (Threat) کیا ہے: ایک دھمکی (threat) ایسا کوئی واقعہ ہے جو کسی اثاثے کو منفی طور پر متاثر کر سکتا ہے- مثال کے طور پر، اگر یہ گم ہو جائے، آف لائن دستک ہو جائے یا کسی غیر مجاز فریق (authorized party) کے ذریعے اس تک رسائی حاصل ہو۔

دھمکیوں (Threat) کو ایسے حالات کے طور پر درجہ بندی کیا جا سکتا ہے جو کسی اثاثے کی رازداری (confidential)، سالمیت (Integrity) یا دستیابی (Availability) سے سمجھوتہ کرتے ہیں، اور یہ جان بوجھ کر یا حادثاتی (accidental) ہو سکتے ہیں۔

جان بوجھ کر دھمکیوں (threat) میں مجرمانہ ہیکنگ یا بدنیتی پر مبنی اندرونی معلومات کی چوری جیسی چیزیں شامل ہوتی ہیں، جب کہ حادثاتی دھمکیوں (threat) میں عام طور پر ملازم کی غلطی، تکنیکی خرابی یا ایسا واقعہ شامل ہوتا ہے جس سے جسمانی نقصان ہوتا ہے، جیسے کہ آگ یا قدرتی آفت۔

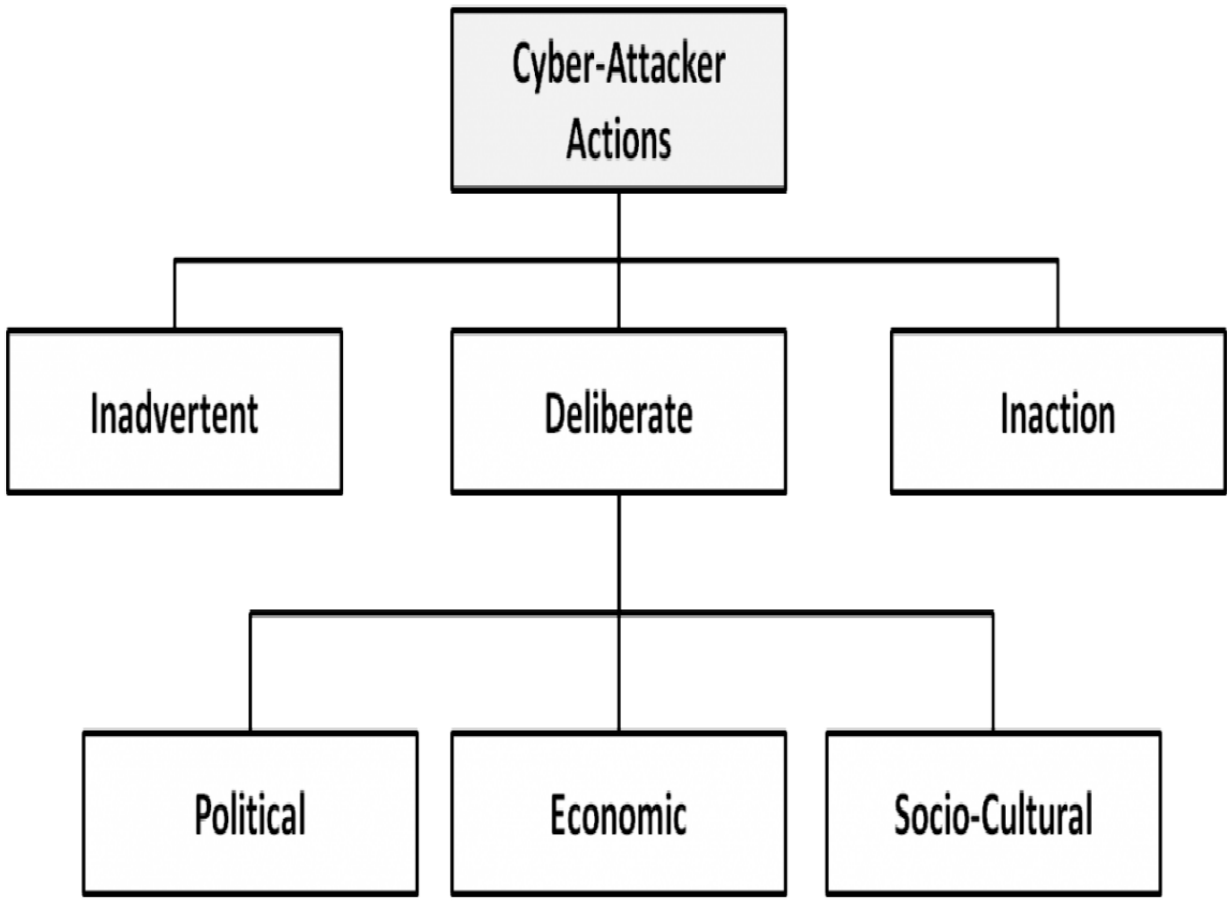
2.3 حملہ آوروں کے محرکات(Motives of attackers)

سائبر حملہ(cyber attack)آوروں کے زمرے ہمیں حملہ آوروں کے محرکات اور ان کے اقدامات کو بہتر طور پر سمجھنے کے قابل بناتے ہیں۔ جیسا کہ تصویر میں دکھایا گیا ہے، آپریشنل سائبر سیکیورٹی(Cyber security)کے خطرات تین قسم کے اقدامات سے پیدا ہوتے ہیں:

سیاسی محرکات(Political motivations): مثالوں میں اہداف کو تباہ کرنا، خلل ڈالنا یا ان پر قابو پانا شامل ہے۔ جاسوسی اور سیاسی بیانات، احتجاج، یا انتقامی کارروائیاں کرنا۔

معاشی محرکات(Economic motivations): مثالوں میں دانشورانہ املاک یا دیگر معاشی طور پر قیمتی اثاثوں کی چوری شامل ہے (مثلاً، فنڈز، کریڈٹ کارڈ کی معلومات)؛ دھوکہ دہی صنعتی جاسوسی اور تخریب کاری؛ اور بلیک میل.

سماجی و ثقافتی محرکات(Socio-cultural motivations): مثالوں میں فلسفیانہ(philosophical)، مذہبی(theological)، سیاسی(political)، اور یہاں تک کہ انسانی اہداف کے ساتھ (Attacks) شامل ہیں۔ سماجی و ثقافتی محرکات(Socio-cultural motivations) میں تفریح(fun)، تجسس(curosity) اور تشہیر یا ان(ego gratification)کی تسکین کی خواہش بھی شامل ہے۔



2.4 حملہ کے اقسام

فعال حملہ(Active attacks):

ایک فعال حملہ(Active attacks)ایک نیٹ ورک کا استحصال ہے جس میں ایک ہیکر ہدف(Hacker target)کے ڈیٹا یا ہدف کے راستے میں ڈیٹا میں تبدیلیاں کرنے کی کوشش کرتا ہے۔

فعال حملوں(Active attacks)کی اقسام:

اس(Attacks)میں، دخل اندازی کرنے والا کسی سسٹم کا مخصوص صارف ہونے کا دکھاوا کرتا ہے تاکہ وہ رسائی حاصل کرے یا اس سے زیادہ مراعات حاصل کرے جس کے لیے وہ مجاز ہیں۔ چوری شدہ لاگ ان آئی ڈیز اور پاس ورڈز کے استعمال کے ذریعے، پروگراموں میں حفاظتی خلاء کو تلاش کرنے کے ذریعے یا تصدیق کے طریقہ کار کو نظرانداز کرنے کے ذریعے ایک نقاب پوش کرنے کی کوشش کی جاسکتی ہے۔

سیشن ری پلے(Session replay): اس قسم کے (Attacks) میں، ایک ہیکر سیشن آئی ڈی چرا کر ایک مجاز صارف کی لاگ ان معلومات چراتا ہے۔ گھسنے والے کو رسائی حاصل ہوتی ہے اور وہ کچھ بھی کرنے کی اہلیت حاصل ہوتی ہے جو ویب سائٹ پر مجاز صارف کر سکتا ہے۔

پیغام میں ترمیم(modification message): اس (Attacks) میں، ایک گھسنے والا پیکٹ ہیڈر ایڈریس (Packet header adder) کو تبدیل کرتا ہے تاکہ پیغام(message) کو کسی مختلف منزل تک پہنچایا جاسکے یا ٹارگٹ مشین پر ڈیٹا میں ترمیم کی جاسکے۔

ایک میں سروس سے انکار (کی) حملہ((denial of service(DoS، صارفین نیٹ ورک(user network)یا ویب وسائل(web resources)تک رسائی سے محروم ہیں۔ یہ عام طور پر ہدف کو سنبھالنے سے زیادہ ٹریفک(traffic)والے ہدف کو مغلوب کرکے پورا کیا جاتا ہے۔

ایک میں تقسیم شدہ انکار کی خدمت((Distributed denial of service (DDoS)استحصال، سمجھوتہ کرنے والے نظاموں کی بڑی تعداد (جسے کبھی کبھی بوٹ نیٹ(Botnet) یا زومبی آرمی(zombie army) کہا جاتا ہے) ایک ہی ہدف پر حملہ کرتے ہیں۔

غیر فعال(Passive attack): غیر فعال(Passive attack)درجہ بندی کے نقطہ نظر سے نسبتاً نایاب(Relatively rare)ہیں، لیکن نسبتاً آسانی(Relatively easy)کے ساتھ انجام دیے جاسکتے ہیں، خاص طور پر اگر ٹریفک(traffic) کو خفیہ نہ کیا گیا ہو۔

فعال حملوں(Active attacks)کی اقسام:-

چھپنا(ٹیپ کرنا)()Eavesdropping (tapping:حملہ(attacker)آور صرف دو اداروں کے ذریعے تبادلہ شدہ پیغامات سنتا ہے۔(Attacks) کے مفید ہونے کے لیے،ٹریفک کو خفیہ نہیں کیا جانا چاہیے۔کوئی بھی غیر خفیہ کردہ معلومات، جیسے کہ HTTPدرخواست کے جواب میں بھیجا گیا پاس ورڈ، حملہ آور کے ذریعے بازیافت کیا جا سکتا ہے۔

ٹریفک تجزیہ(Traffic analysis):حملہ(attack)آور ٹریفک(traffic)میں منتقل ہونے والے میٹاڈیٹا(meta-data)کو دیکھتا ہے تاکہ تبادلے اور شرکت کرنے والے اداروں سے متعلق معلومات کا اندازہ لگایا جا سکے، جیسے تبادلہ ٹریفک(traffic) کی شکل (ریٹ، مدت، وغیرہ)۔ان صورتوں میں جہاں خفیہ کردہ ڈیٹا استعمال کیا جاتا ہے،ٹریفک(traffic) تجزیہ بھی حملوں(attack) کی قیادت کر سکتے ہیں(cryptanalysis) جس کے ذریعے حملہ(attack)آور معلومات حاصل کر سکتا ہے یاٹریفک(traffic)کو غیر خفیہ کرنے میں کامیاب ہو سکتا ہے۔

سافٹ ویئر (Software Attacks): بدنیتی پر مبنی کوڈ(Malicious code) (کبھی کبھی کہا جاتا ہے۔ میلویئر)malware() ایک قسم کا سافٹ ویئر (software)ہے جو صارف کے علم یا منظوری کے بغیر، کمپیوٹر صارف (computer user)کے آپریٹنگ سسٹم(operating system)پر قبضہ کرنے یااسے نقصان پہنچانے کے لیے ڈیزائن کیا گیا ہے۔اسے ہٹانا بہت مشکل اور بہت نقصان دہ ہو سکتا ہے۔

میلویئر کی عام مثالیں درج ذیل جدول میں درج ہیں۔

حملہ(attack)	خصوصیات(Features)
وائرس(Virus)	اے وائرس ایک ایسا پروگرام ہے جو کمپیوٹر سسٹم کو نقصان پہنچانے اور خود کو دوسرے کمپیوٹر سسٹم میں نقل کرنے کی کوشش کرتا ہے۔ایک وائرس: نقل تیار(Replicate) کرنے کے لیے ایک میزبان(Host) کی ضرورت ہوتی ہے اور عام طور پر خود کو میزبان فائل یا ہارڈ ڈرائیو سیکٹر سے منسلک کرتا ہے۔ ہر بار جب میزبان(host)استعمال ہوتا ہے تو نقل کرتا ہے۔ اکثر ڈیٹا کی تباہی یا بدعنوانی(Corruption)پر توجہ مرکوز کرتا ہے۔ عام طور پر عملدرآمد(Implementation)کی صلاحیتوں کے ساتھ فائلوں سے منسلک ہوتا ہے جیسے .exe،doc. ،اور.batایکسٹینشن((Extension۔ اکثر ای میل(Email)کے ذریعے تقسیم کیا جاتا ہے۔بہت سے وائرس آپ کی ایڈریس بک میں موجود ہر کسی کو خود کو ای میل کر سکتے ہیں۔ مثالیں:سٹونڈ،مائیکل اینجلو،میلیسا،I Love You۔

Worm	ایک خود ساختہ (Self-made) پروگرام ہے جسے کسی بھی کام کے لیے ڈیزائن (design) کیا جا سکتا ہے، جیسے فائلوں کو حذف (delete) کرنا یا ای میل (email) کے ذریعے دستاویزات (documents) بھیجنا۔ ایک worm اپنے آپ کو نقل کرنے کے عمل میں نیٹ ورک ٹریفک (network traffic) پر منفی اثر ڈال سکتا ہے۔ Worm: متاثرہ کمپیوٹر میں بیک ڈور (backdoor) انسٹال کر سکتے ہیں۔ عام طور پر کمزوری کے ذریعے سسٹم میں متعارف کرایا جاتا ہے۔ ایک سسٹم کو متاثر کرتا ہے اور نیٹ ورک کے دوسرے سسٹمز میں پھیلتا ہے۔ مثال: کوڈ ریڈ Code Red۔
Trojen Horse	ایک بدنیتی (Malice) پر مبنی پروگرام ہے جو جائز سافٹ ویئر (software) کے بھیس میں ہے۔ صحیح سوجھ بوجھ کا ماحول اکثر زیادہ کمزور اور ٹروجن ہارس (Trojan horse) کے حملوں (attacker) کے لیے حساس ہوتی ہے کیونکہ سیکیورٹی صارف پر مرکوز اور صارف (user-centric) کی ہدایت پر ہوتی ہے۔ اس طرح صارف (user) کے اکاؤنٹ کا سمجھوتہ پورے ماحول کے سمجھوتہ کا باعث بن سکتا ہے۔ Trojen Horse: خود کو نقل نہیں کر سکتا۔ اکثر جاسوسی کے فنکشنز (جیسے پیکٹ سنیفر) یا بیک ڈور فنکشنز (backdoor function) پر مشتمل ہوتے ہیں جو کمپیوٹر کو نیٹ ورک سے دور سے کنٹرول کرنے کی اجازت دیتے ہیں۔ اکثر مفید سافٹ ویئر جیسے screen saver یا گیمز میں چھپا ہوتا ہے۔ مثال: Back Orifice, Net Bus, Wack-a-Mole.
Logic Bomb	Malware ہے جو متحرک ہونے تک غیر فعال رہتا ہے۔ لاجک بم (Logic Bomb) غیر متزلزل (Attacks) کی ایک مخصوص مثال ہے۔ ایک محرک سرگرمی ایک مخصوص تاریخ اور وقت، ایک مخصوص پروگرام کا آغاز، یا کسی مخصوص قسم کی سرگرمی کی پروسیسنگ ہو سکتی ہے۔ لاجک بم خود نقل نہیں کرتے۔

2.5 ہارڈ ویئر حملوں (Hardware attacks)

عام ہارڈ ویئر حملوں (Hardware attacks) میں شامل ہیں: میلویئر (Malware) یا دوسرے داخلی مقاصد کے لیے

بیک ڈور(backdoor)تیار کرنا؛ پچھلے دروازے صرف سافٹ ویئر(software)اور ہارڈ ویئر(hardware)تک ہی محدود نہیں ہیں، بلکہ وہ ایمبیڈڈ ریڈ(Embedded Red) یو فریکوئنسی(frequency) شناخت (RFID) چپس اور میموری(memory)کو بھی متاثر کرتے ہیں۔

دوسرے ہارڈ ویئر(hardware)کو کھولے بغیر محفوظ میموری تک رسائی حاصل کر کے چھپنا

خرابیاں پیدا کرنا، معمول کے رویے میں رکاوٹ پیدا کرنا

ناگوار کارروائیوں(Invasive actions)کے ساتھ ہارڈ ویئر(hardware)میں ترمیم کی چھیڑ چھاڑ

Backdoor کی تخلیق؛عام کمپیوٹر کی توثیق(verification)کے نظام کو نظرانداز کرنے کے لیے پوشیدہ طریقوں کی موجودگی

جعل سازی کرنے والے پروڈکٹ اثاثے(Product assets)جو غیر معمولی آپریشنز(Operations)اور

سسٹمز(systems)تک نقصان دہ رسائی حاصل کرنے کے لیے بنائے گئے ہیں۔

سائبر تھریٹس-سائبر وارفیئر(Cyber Threats - Cyber Warfare):

سائبر وارفیئر(Cyber Warfare)سے مراد ڈیجیٹل حملوں(Digita attack)کا استعمال ہے- جیسے کمپیوٹر وائرس (computer virus)اور ہیکنگ(hanging)--ایک ملک کی طرف سے دوسرے ملک کے اہم کمپیوٹر سسٹم میں خلل ڈالنے کے لئے، جس کا مقصد نقصان، موت اور تباہی پیدا کرنا ہے۔ مستقبل کی جنگوں(Wars)میں دشمن کے بنیادی ڈھانچے(Structures)پر حملہ(attack)کرنے کے لیے کمپیوٹر کوڈ (computer code)کا استعمال کرتے ہوئے ہیکرز(hackers)، بندوقوں اور میزائلوں جیسے روایتی ہتھیاروں(traditional weapons)کا استعمال کرتے ہوئے فوجیوں کے ساتھ مل کر لڑتے ہوئے دیکھیں گے۔

سائبر جنگ(cyber war)میں ایک قومی ریاست یا بین الاقوامی تنظیم(international system)کی طرف سے حملہ(attack)کرنا اور کسی دوسرے ملک کے کمپیوٹرز یا معلوماتی نیٹ ورکس کو نقصان پہنچانے کی کوشش شامل ہے، مثال کے طور پر، کمپیوٹر وائرس یا سروس سے انکار کے(Attacks)۔

سائبر کرائم(Cyber crime):سائبر کرائم(cyber crime)ایک مجرمانہ(Criminal)سرگرمی ہے جو یا تو کمپیوٹر، کمپیوٹر نیٹ ورک(computer network)یا نیٹ ورک ڈیوائس (network device)کو نشانہ بناتی(targeting)ہے یا استعمال کرتی ہے۔سائبر کرائم(cyber crime)افراد یا تنظیموں(Individuals or organizations)کے ذریعہ انجام دیا جاتا ہے۔

کچھ سائبر جرائم(Cybercrime)پیشہ افراد منظم ہوتے ہیں، جدید تکنیکوں(techniques)کا استعمال کرتے ہیں اور انتہائی تکنیکی طور پر ہنر مند ہوتے ہیں۔دوسرے نئے ہیکرز ہیں۔

سائبر دہشت گردی(Cyber terrorism): -سائبر دہشت گردی(Cyber terrorism) سائبر

اسپیس(Cyberspace) اور دہشت گردی(terrorism). اس سے مراد کمپیوٹرز، نیٹ ورکس(computer networks)اور ان میں محفوظ کردہ معلومات کے خلاف غیر قانونی حملوں(attacks)اور حملوں کی دھمکیاں (Threats of attacks)ہیں جب کسی حکومت یا اس کے لوگوں کو سیاسی یا سماجی مقاصد کے حصول کے لیے ڈرانے یا مجبور کرنے کے لیے کیا جاتا ہے۔

مثالیں :- کمپیوٹر سسٹم(computer system) کو ہیک(hack) کرنا، کمزور نیٹ ورکس(networks) میں وائرس (virus)متعارف کروا رہے ہیں، ویب سائٹ(website) کو ڈیفیس کر رہے ہیں، سروس(service) سے انکار کر رہے ہیں، یا الیکٹرانک کمیونیکیشن(electronic communication)کے ذریعے دہشت گردی کے خطرات پیدا کر رہے ہیں۔

سائبر جاسوسی(Cyber Espionage):- معلومات کے حامل کی اجازت اور علم کے بغیر راز اور معلومات حاصل کرنے کا عمل ہے افراد، حریف، گروہ، حکومتیں اور دشمن ذاتی(personal enemy)، معاشی(Economic)، سیاسی(Political) یا فوجی فائدے کے لیے انٹرنیٹ(internet)پر طریقے استعمال کرتے ہیں۔

2.6 سیکورٹی پالیسیاں(Security policies)

سیکیورٹی پالیسیاں(Security policies) قواعد کا ایک رسمی مجموعہ ہیں جو کسی تنظیم(organisation)کی طرف سے اس بات کو یقینی بنانے کے لیے جاری کیا جاتا ہے کہ وہ صارف جو کمپنی کی ٹیکنالوجی (technology)اور معلوماتی اثاثوں (Information assets)تک رسائی کے مجاز ہیں معلومات کی حفاظت سے متعلق قواعد وضوابط کی تعمیل کرتے ہیں۔



سیکیورٹی پالیسی (security policy) کو "زندہ دستاویز" بھی سمجھا جاتا ہے جس کا مطلب ہے کہ دستاویز کبھی ختم نہیں ہوتی، لیکن اسے ٹیکنالوجی(technology) کی ضروریات اور ملازمین کی تبدیلیوں کے مطابق مسلسل اپ ڈیٹ کیا جاتا ہے۔

ہم اپنے نیٹ ورک کی سیکیورٹی(security) کو منظم کرنے کے لیے سیکیورٹی پالیسیوں(security policy)کا استعمال کرتے ہیں۔ زیادہ تر قسم کی سیکیورٹی پالیسیاں(security policy)انسٹالیشن کے دوران خود بخود بن جاتی ہیں۔ ہم اپنے مخصوص ماحول کے مطابق پالیسیوں(policy) کو بھی اپنی مرضی کے مطابق بنا سکتے ہیں۔

سیکورٹی پالیسیوں کی ضرورت(Need)-

- اس سے کارکردگی میں اضافہ ہوتا ہے۔

- یہ نظم وضبط اور احتساب کو برقرار رکھتا ہے۔
- یہ کاروباری معاہدہ کر سکتا ہے یا توڑ سکتا ہے۔
- یہ ملازمین کو حفاظتی خواندگی کے بارے میں تعلیم دینے میں مدد کرتا ہے۔

سائبر سیکیورٹی (Cyber security) پالیسیوں (policies) کی کچھ اہم سفارشات (recommendations) ذیل میں بیان کی گئی ہیں۔

وائرس اور اسپائی ویئر (Spyware) کے تحفظ کی پالیسی (policies): یہ فائلوں میں تھریڈز (threads) کا پتہ لگانے میں مدد کرتا ہے، مشکوک رویے کی نمائش کرنے والی ایپلی کیشنز (applications) کا پتہ لگانے میں۔

دستخطوں (Signatures) کا استعمال کر کے وائرس (virus) کے مضر اثرات (Side effects) اور حفاظتی خطرات کو ہٹانا اور مرمت کرتا ہے۔

فائروال پالیسی (Firewall Policy): یہ غیر مجاز صارفین (unauthorized user) کو انٹرنیٹ سے جڑنے والے سسٹمز اور نیٹ ورکس تک رسائی سے روکتا ہے۔

یہ سائبر کرائمینلز (cyber criminal) کے حملوں (attacks) کا پتہ لگاتا ہے اور نیٹ ورک ٹریفک (network traffic) کے ناپسندیدہ ذرائع کو ہٹاتا ہے۔

مداخلت کی روک تھام کی پالیسی (Intrusion Prevention Policy):

یہ پالیسی نیٹ ورک (policy network) کے حملوں (attacks) اور براؤزر حملوں (browser attacks) کا خود بخود پتہ لگاتی ہے اور اسے روکتی ہے۔

یہ ایپلی کیشنز (applications) کو کمزوریوں سے بھی بچاتا ہے اور ایک یا زیادہ ڈیٹا پیکجز (data packages) کے مواد کو چیک کرتا ہے اور قانونی طریقوں سے آنے والے میلویئر (malware) کا پتہ لگاتا ہے۔

ایپلیکیشن اور ڈیوائس کنٹرول (Application and device control):

یہ پالیسی سسٹم کے وسائل (resources) کو ایپلی کیشنز سے بچاتی ہے اور ان پیریفرل (peripheral) ڈیوائسز کا انتظام کرتی ہے جو سسٹم سے منسلک ہو سکتے ہیں۔

ڈیوائس کنٹرول پالیسی (Device control policy) ونڈوز اور میک دونوں کمپیوٹرز پر لاگو ہوتی ہے جبکہ ایپلیکیشن کنٹرول پالیسی صرف ونڈوز کلائنٹس (windows clients) پر لاگو کی جا سکتی ہے۔

2.7 اکتسابی نتائج

- Assets اور Threats کے تصور کو سمجھ سکے گا۔

- Attackers کے مختلف motives کی وضاحت کر سکے گا۔
- Activeاور Passive Attacks میں فرق کر سکے گا۔
- مختلف Software اور Hardware Attacks کو سمجھ سکے گا۔
- Cyber Warfare،Cyber Crime، Cyber Terrorismاور Cyber Espionage کی وضاحت کر سکے گا۔
- Security Policies کی اہمیت اور مختلف اقسام کو بیان کر سکے گا۔

2.8 کلیدی الفاظ

- اثاثہ **Asset** —
- خطرہ **Threat** —
- حملہ آور **Attacker** —
- فعال حملہ **Active Attack** —
- غیر فعال حملہ **Passive Attack** —
- Session Replay
- Message Modification
- DoS
- DDoS
- Eavesdropping
- Traffic Analysis
- Software Attack
- Virus
- Worm
- Trojan Horse
- Logic Bomb
- Hardware Attack
- Cyber Warfare

- Cyber Crime
- Cyber Terrorism

2.9 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات

1۔ اثاثہ (Asset) کیا ہے؟

2۔ خطرہ (Threat) کیا ہے؟

3۔ سائبر کرائم (Cyber Crime) کیا ہے؟

4۔ سائبر جاسوسی (Cyber Espionage) کیا ہے؟

5۔ سیکیورٹی پالیسی (Security Policy) کیا ہے؟

مختصر جوابات کے حامل سوالات

1۔ اثاثہ (Asset) اور خطرہ (Threat) سے کیا مراد ہے؟ مثالوں کے ساتھ وضاحت کریں۔

2۔ سائبر حملہ آوروں کے مختلف محرکات (Motives of Attackers) کی وضاحت کریں۔

3۔ فعال حملوں (Active Attacks) کی اقسام کی وضاحت کریں۔

4۔ غیر فعال حملوں (Passive Attacks) کی وضاحت کریں۔ Eavesdropping اور Traffic Analysis کو بیان کریں۔

5۔ Software Attacks کیا ہیں؟ Virus ، Wormاور Trojan Horse کی وضاحت کریں۔

6۔ Hardware Attacks کیا ہیں؟ مختلف Hardware Attacks کی وضاحت کریں۔

7۔ Cyber Warfare، Cyber Crimeاور Cyber Terrorism میں فرق بیان کریں۔

8۔ Security Policy کیا ہے؟ اس کی ضرورت اور اہمیت بیان کریں۔

طویل جوابات کے حامل سوالات

1۔ اثاثہ (Asset) اور خطرہ (Threat) کی تفصیل سے وضاحت کریں۔ خطرات کی مختلف اقسام اور ان کے اثرات کو مثالوں کے ساتھ بیان کریں۔

2۔ سائبر حملوں کی مختلف اقسام کی تفصیل سے وضاحت کریں۔ Active Attacks اور Passive Attacks میں فرق بیان کرتے ہوئے ان کی مختلف اقسام کی وضاحت کریں۔

3۔ سیکیورٹی پالیسی (Security Policy) کیا ہے؟اس کی ضرورت،اہمیت اور مختلف Security Policies جیسے Intrusion Prevention ،Firewall Policy،Virus & Spyware Protection Policy اور Application & Device Control Policy کی تفصیل سے وضاحت کریں۔

2.10 تجویز کردہ اکتسابی مواد

1۔ Assets and Threats

2۔ Motives of Attackers

3۔ Types of Attacks

4۔ Active and Passive Attacks

5۔ Software Attacks

6۔ Hardware Attacks

7۔ Cyber Warfare

8۔ Cyber Crime

9۔ Cyber Terrorism

10۔ Cyber Espionage

11۔ Security Policies

12۔ Firewall Policy

13۔ Intrusion Prevention Policy

14۔ Application and Device Control

اکائی 3۔ سائبر جرائم اور روک تھام

(Cybercrimes and Prevention)

اکائی کے اجزاء

3.0 تمہید

3.1 مقاصد

3.2 سائبر جرائم کا تعارف(Introduction to Cybercrime)

3.3 سائبر جرائم کی اقسام(Types of Cybercrimes)

3.4 مجرم کیسے حملوں کی منصوبہ بندی کرتے ہیں(How do criminals plan attacks)۔

3.5 سائبر اسٹاکنگ اور حفاظتی نکات(Cyberstalking and safety tips)

3.6 سوشل انجینئرنگ اور اس کے اثرات(Social engineering and its effects)

3.7 سائبر کیفے اور سائبر کرائمز(Cyber Cafes and Cybercrimes)

3.8 سائبر کیفے میں سائبر کرائمز کا ارتکاب کیسے کیا جاتا ہے

(How cybercrimes are committed in cyber cafes)

3.9 حقیقی دنیا کے سائبر کرائم کیسز(Real-world cybercrime cases)

3.10 قانونی فریم ورک اور سائبر کرائم قوانین(Legal framework and cybercrime laws)

3.11 سائبر کرائمز کے خلاف حفاظتی اقدامات(Safeguards against cybercrimes)

3.12 سائبر سیکیورٹی کے لیے بہترین طریقے(Best practices for cyber security)

3.13 نتیجہ(Conclusion)

3.14 اکتسابی نتائج

3.15 کلیدی الفاظ

3.16 نمونہ امتحانی سوالات

3.17 تجویز کردہ اکتسابی مواد

3.0 تمہید

سائبر جرائم ڈیجیٹل نیٹ ورکس پر کی جانے والی غیر قانونی سرگرمیوں کا ایک وسیع مجموعہ ہیں۔ ان میں شناخت کی چوری، فشنگ، سائبر اسٹاکنگ اور مالی فراڈ شامل ہیں۔ ڈیجیٹل ٹیکنالوجی کے بڑھتے ہوئے استعمال کے ساتھ سائبر جرائم میں بھی اضافہ ہوا ہے۔ سائبر مجرم سسٹمز، نیٹ ورکس اور انسانی نفسیات کی کمزوریوں کا فائدہ اٹھاتے ہیں۔ سائبر جرائم مالی نقصان کے علاوہ ذاتی رازداری، کاروباری استحکام اور قومی سلامتی کے لیے بھی خطرہ بن سکتے ہیں۔

3.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- سائبر جرائم کے بنیادی تصور کو سمجھ سکے گا۔
- سائبر جرائم کی مختلف اقسام کی وضاحت کر سکے گا۔
- یہ سمجھ سکے گا کہ سائبر مجرم حملوں کی منصوبہ بندی کیسے کرتے ہیں۔
- سائبر اسٹاکنگ اور اس سے بچاؤ کے طریقوں کو سمجھ سکے گا۔
- سوشل انجینئرنگ اور اس کے اثرات کی وضاحت کر سکے گا۔
- سائبر کیفے سے متعلق سائبر جرائم اور خطرات کو سمجھ سکے گا۔
- حقیقی دنیا کے سائبر کرائم کیسز کا مطالعہ کر سکے گا۔
- سائبر کرائم سے متعلق قانونی فریم ورک اور قوانین کو سمجھ سکے گا۔
- سائبر جرائم سے بچاؤ کے حفاظتی اقدامات اور سائبر سیکیورٹی کے بہترین طریقوں کو بیان کر سکے گا۔

3.2 سائبر جرائم کا تعارف (Introduction to Cybercrime)

سائبر جرائم ڈیجیٹل نیٹ ورکس پر کی جانے والی غیر قانونی سرگرمیوں کی ایک وسیع رینج کو گھیرے ہوئے ہیں۔ ان جرائم میں شناخت کی چوری، فشنگ، سائبر اسٹاکنگ اور مالی فراڈ شامل ہیں۔ ہر شعبے میں تیزی سے ڈیجیٹل تبدیلی کے ساتھ، سائبر جرائم کے پھیلاؤ میں اضافہ ہوا ہے، جس کے لیے مضبوط حفاظتی اقدامات اور بیداری کی ضرورت ہے۔

سائبر جرائم پیشہ افراد اپنے حملوں کو انجام دینے کے لیے سسٹمز، نیٹ ورکس اور انسانی نفسیات میں موجود کمزوریوں کا استحصال کرتے ہیں۔ یہ جرائم مالی فائدے، سیاسی مقاصد، ذاتی انتقام، یا محض خلل ڈالنے کے لیے کیے جا سکتے ہیں۔ سائبر جرائم نہ صرف مالی نقصان کا باعث بنتے ہیں بلکہ قومی سلامتی، کارپوریٹ استحکام اور ذاتی رازداری کو بھی خطرات لاحق ہوتے ہیں۔

3.3 سائبر جرائم کی اقسام(Types of Cybercrimes)

سائبر جرائم کو ان کے اثرات اور پھانسی کے طریقوں کی بنیاد پر درجہ بندی کیا جا سکتا ہے:

A. مالیاتی سائبر کرائمز

- آن لائن فراڈ، فشنگ گھوٹالے، اور بینکنگ فراڈ۔
- کریڈٹ کارڈ کی معلومات کی چوری.
- رینسم ویئر حملے متاثرین سے رقم کا مطالبہ کرتے ہیں۔

B. سائبر دہشت گردی

- حملے جن کا مقصد اہم انفراسٹرکچر (مثلاً پاور گرڈز، مالیاتی ادارے) میں خلل ڈالنا ہے۔
- خوف اور تشدد کو ہوا دینے کے لیے پروپیگنڈا پھیلانا۔

C. سائبر جاسوسی

- درجہ بند سرکاری یا کارپوریٹ ڈیٹا تک غیر مجاز رسائی۔
- حریفوں یا سیاسی اداروں کی جاسوسی کرنا۔

D. سائبر دھونس اور سائبر اسٹاکنگ

- ڈیجیٹل پلیٹ فارمز پر ہراساں کرنا، دھمکیاں دینا اور بلیک میل کرنا۔
- دھوکہ دہی کے لیے جعلی پروفائلز کا استعمال۔

E. ہیکنگ اور ڈیٹا کی خلاف ورزیاں

- ذاتی، کارپوریٹ، یا سرکاری نیٹ ورکس تک غیر مجاز رسائی۔
- ڈارک ویب پر چوری شدہ ڈیٹا بیچنا۔

3.4 مجرم کیسے حملوں کی منصوبہ بندی کرتے ہیں(How do criminals plan attacks)

سائبر کرائمین اپنے جرائم کو انجام دینے کے لیے ایک منظم انداز اختیار کرتے ہیں۔ان کے طریقہ کار میں شامل ہیں:

A. پہچان

- غیر فعال اور فعال نگرانی کے ذریعے ہدف کے بارے میں معلومات جمع کرنا۔

B. استحصال

- کمزور پاس ورڈز، بغیر پیچ شدہ سافٹ ویئر، اور سوشل انجینئرنگ جیسی کمزوریوں کا استعمال۔

C. پھانسی

- حملہ شروع کرنا، چاہے میلویئر، فشنگ، یا براہ راست سسٹم کی خلاف ورزیوں کے ذریعے۔

3.5 سائبر اسٹالنگ اور حفاظتی نکات

A. سائبر اسٹاکنگ کی تعریف اور اثر (Definition and impact of cyberstalking)

- سائبر اسٹاکنگ میں کسی فرد کو ہراساں کرنے، دھمکانے یا دھمکانے کے لیے الیکٹرانک مواصلات کا بار بار استعمال شامل ہے۔

B. سائبر اسٹاکنگ کے عام طریقے (Common Methods of Cyberstalking)

- سوشل میڈیا کی سرگرمیوں کی نگرانی۔
- دھمکیاں بھیجنا یا ہراساں کرنے والی ای میلز۔
- آن لائن سرگرمیوں کی پیروی کرنے کے لیے ٹریکنگ سافٹ ویئر کا استعمال۔

C. روک تھام کی تکنیک (Prevention Techniques)

- سوشل میڈیا پر مضبوط رازداری کی ترتیبات استعمال کریں۔
- ذاتی تفصیلات کو عوامی طور پر شیئر کرنے سے گریز کریں۔
- مشکوک رابطوں کی اطلاع دیں اور بلاک کریں۔

3.6 سوشل انجینئرنگ اور اس کے اثرات (Social engineering and its effects)

سوشل انجینئرنگ خفیہ معلومات کو ظاہر کرنے کے لیے افراد کی ہیرا پھیری ہے۔ حملہ آور تکنیکی کمزوریوں کے بجائے انسانی نفسیات کا استحصال کرتے ہیں۔

A. سوشل انجینئرنگ حملوں کی اقسام (Types of social engineering attacks)

- فشنگ - جعلی ای میلز جو صارف کی اسناد چرانے کے لیے بنائی گئی ہیں۔
- بہانہ کرنا - اعتماد حاصل کرنے کے لیے اتھارٹی کے اعداد و شمار کی نقالی کرنا۔
- بیت کرنا - متاثرین کو ایسی پیشکشوں کے ساتھ راغب کرنا جو میلویئر ڈاؤن لوڈز کا باعث بنتے ہیں۔
- ٹیلگیٹنگ - محفوظ علاقوں تک غیر مجاز جسمانی رسائی حاصل کرنا۔

B. روک تھام کی حکمت عملی (Prevention strategies)

- درخواستوں کا جواب دینے سے پہلے بھیجنے والوں کی تصدیق کریں۔
- نامعلوم لنکس پر کلک کرنے سے گریز کریں۔

- ملازمین اور افراد کو سائبر سیکیوریٹی بیداری کے بارے میں تعلیم دیں۔

3.7 سائبر کیفے اور سائبر کرائمز (Cyber Cafes and Cybercrimes)

پبلک انٹرنیٹ کیفے اکثر غیر محفوظ نیٹ ورکس اور مشترکہ کمپیوٹرز کی وجہ سے سائبر جرائم کی سرگرمیوں کے لیے ہاٹ سپاٹ بن جاتے ہیں۔

A. سائبر کیفے میں خطرات

- غیر محفوظ وائی فائی نیٹ ورکس۔
- عوامی طور پر قابل رسائی کمپیوٹرز جن میں میلویئر انسٹال ہو سکتا ہے۔

B. احتیاطی تدابیر

- ورچوئل پرائیویٹ نیٹ ورکس (VPNs) استعمال کریں۔
- پبلک کمپیوٹرز سے حساس اکاؤنٹس میں لاگ ان کرنے سے گریز کریں۔
- ہر سیشن کے بعد براؤزنگ کی تاریخ اور کیش صاف کریں۔

3.8 سائبر کیفے میں سائبر کرائمز کا ارتکاب کیسے کیا جاتا ہے

(How cybercrimes are committed in cyber cafes)

سائبر کرائمین سائبر کیفے کے صارفین کا استحصال کرنے کے لیے مختلف طریقوں سے فائدہ اٹھاتے ہیں:

- کی لاگنگ: اسناد چوری کرنے کے لیے کی اسٹروکس کو ٹریک کرنا۔
- سیشن ہائی جیکنگ: کنٹرول حاصل کرنے کے لیے صارف کے سیشن کو روکنا۔
- وائی فائی سنفنگ: عوامی Wi-Fi پر منتقل کردہ ڈیٹا کیپچر کرنا۔

3.9 حقیقی دنیا کے سائبر کرائم کیسز (Real-World Cybercrime Cases)

WannaCry Ransomware Attack) 2017): ایک عالمی رینسم ویئر حملہ جس نے کاروبار اور سرکاری ایجنسیوں کو متاثر کیا۔

Yahoo ڈیٹا کی خلاف ورزی (2013-2014): کمزور سیکورٹی پروٹوکول کی وجہ سے 3 بلین سے زائد صارف اکاؤنٹس سے سمجھوتہ کیا گیا۔

3.10 قانونی فریم ورک اور سائبر کرائم قوانین

A. بین الاقوامی سائبر کرائم قوانین

- جنرل ڈیٹا پروٹیکشن ریگولیشن (GDPR)-یورپ
- کمپیوٹر فراڈ اینڈ ابیوز ایکٹ USA - (CFAA)

B. ہندوستانی سائبر قوانین

- انفارمیشن ٹیکنالوجی ایکٹ، 2000 (آئی ٹی ایکٹ 2000)
- انڈین پینل کوڈ (IPC) سائبر جرائم سے متعلق سیکشنز

3.11 سائبر کرائمز کے خلاف حفاظتی اقدامات

- باقاعدہ سافٹ ویئر اپ ڈیٹس اور سیکیورٹی پیچ۔
- تمام اکاؤنٹس کے لیے مضبوط، منفرد پاس ورڈ استعمال کریں۔
- ملٹی فیکٹر توثیق (MFA) کو فعال کریں۔
- ای میل منسلکات اور نامعلوم لنکس سے محتاط رہیں۔

3.12 سائبر سیکیورٹی کے لیے بہترین طریقے

- سائبر سیکیوریٹی بیداری کے بارے میں افراد کو تعلیم دیں۔
- تنظیموں میں سخت رسائی کنٹرول کے اقدامات کو نافذ کریں۔
- غیر معمولی رویے کے لیے نیٹ ورک کی سرگرمی کو باقاعدگی سے مانیٹر کریں۔
- حساس ڈیٹا کے لیے خفیہ کاری کا استعمال کریں۔

3.13 نتیجہ

سائبر جرائم افراد، کاروباری اداروں اور حکومتوں کے لیے بڑھتے ہوئے خطرہ بن گئے ہیں۔ سائبر کرائمز کی مختلف اقسام کو سمجھنا، مجرم کیسے حملوں کو انجام دیتے ہیں، اور بہترین حفاظتی اقدامات خطرات کو نمایاں طور پر کم کر سکتے ہیں۔ سائبر سیکیورٹی کے مناسب طریقوں اور قانونی فریم ورک کی پابندی کے ساتھ، افراد اور تنظیمیں ایک محفوظ ڈیجیٹل ماحول بنا سکتے ہیں۔

تکنیکی ترقی کے اس دور میں، ابھرتے ہوئے سائبر خطرات سے چوکنا رہنا اور باخبر رہنا بہت ضروری ہے۔ سائبر سیکیوریٹی ایک مشترکہ ذمہ داری ہے، اور ہر شخص کو ذاتی اور پیشہ ورانہ ڈیجیٹل اثاثوں کی حفاظت کے لیے ضروری احتیاطی تدابیر اختیار کرنی چاہئیں۔

3.14 اکتسابی نتائج

- سائبر جرائم کی تعریف اور اہمیت بیان کر سکے گا۔
- مالیاتی سائبر کرائمز، سائبر دہشت گردی، سائبر جاسوسی، سائبر دھونس، سائبر اسٹاکنگ اور ہیکنگ کی وضاحت کر سکے گا۔
- سائبر مجرموں کے حملوں کی منصوبہ بندی کے مراحل بیان کر سکے گا۔
- سائبر اسٹاکنگ کے عام طریقوں اور حفاظتی اقدامات کو سمجھ سکے گا۔
- سوشل انجینئرنگ کی مختلف اقسام جیسے Phishing، Pretexting، Baiting اور Tailgating کی وضاحت کر سکے گا۔
- سائبر کیفے میں موجود خطرات اور جرائم کے طریقوں کو سمجھ سکے گا۔
- WannaCry اور Yahoo Data Breach جیسے حقیقی سائبر کرائم کیسز کو بیان کر سکے گا۔
- سائبر کرائم سے متعلق قانونی فریم ورک کی بنیادی معلومات حاصل کر سکے گا۔
- سائبر جرائم سے بچاؤ کے لیے حفاظتی اقدامات اور Best Practices بیان کر سکے گ

3.15 کلیدی الفاظ

- سائبر کرائم — Cybercrime
- مالیاتی سائبر کرائم — Financial Cybercrime
- سائبر دہشت گردی — Cyber Terrorism
- سائبر جاسوسی — Cyber Espionage
- سائبر دھونس — Cyberbullying
- سائبر اسٹاکنگ — Cyberstalking
- ہیکنگ — Hacking
- فشنگ — Phishing
- سوشل انجینئرنگ — Social Engineering
- بہانہ کرنا — Pretexting
- بیت کرنا — Baiting
- ٹیلگیٹنگ — Tailgating

- کی لاگنگ Keylogging —
- سیشن ہائی جیکنگ Session Hijacking —
- Wi-Fi Sniffing
- رینسم ویئر Ransomware —
- GDPR

3.16 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات

1۔ سائبر کرائم سے کیا مراد ہے؟

2۔ سائبر اسٹاکنگ کیا ہے؟

3۔ سوشل انجینئرنگ کیا ہے؟

4۔ فشنگ (Phishing) کیا ہے؟

5۔ سائبر جاسوسی (Cyber Espionage) کیا ہے؟

مختصر جوابات کے حامل سوالات

1۔ سائبر جرائم کی مختلف اقسام کی وضاحت کریں۔

2۔ سائبر مجرم حملوں کی منصوبہ بندی کیسے کرتے ہیں؟ وضاحت کریں۔

3۔ سائبر اسٹاکنگ کیا ہے؟ اس کے عام طریقے اور حفاظتی اقدامات بیان کریں۔

4۔ سوشل انجینئرنگ کیا ہے؟ اس کی مختلف اقسام کی وضاحت کریں۔

5۔ سائبر کیفے میں موجود سائبر سیکیورٹی کے خطرات اور احتیاطی تدابیر بیان کریں۔

6۔ سائبر کیفے میں سائبر جرائم کس طرح کیے جاتے ہیں؟ وضاحت کریں۔

7۔ حقیقی دنیا کے سائبر کرائم کیسز WannaCry Ransomware Attack اور Yahoo Data Breach کی وضاحت کریں۔

8۔ سائبر جرائم کے خلاف حفاظتی اقدامات اور سائبر سیکیورٹی کے بہترین طریقے بیان کریں۔

طویل جوابات کے حامل سوالات

1۔ سائبر کرائم کی تعریف بیان کرتے ہوئے سائبر جرائم کی مختلف اقسام، ان کے مقاصد اور معاشرے پر ان کے اثرات کی تفصیل سے

وضاحت کریں۔

2۔ سوشل انجینئرنگ کیا ہے؟Phishing، Pretexting، Baitingاور Tailgating کی تفصیل بیان کرتے ہوئے ان سے بچاؤ کی حکمت عملیوں کی وضاحت کریں۔

3۔ سائبر کرائم کے خلاف قانونی فریم ورک اور حفاظتی اقدامات کی تفصیل سے وضاحت کریں۔GDPR، CFAA، IT Act 2000، مضبوط پاس ورڈز، MFA، سافٹ ویئر اپ ڈیٹس اور دیگر Best Practices کو بیان کریں۔

3.17 تجویز کردہ اکتسابی مواد

1۔ سائبر جرائم کا تعارف(Introduction to Cybercrime)

2۔ سائبر جرائم کی اقسام (Types of Cybercrimes)

3۔ سائبر مجرموں کی جانب سے حملوں کی منصوبہ بندی

4۔ سائبر اسٹاکنگ اور حفاظتی نکات

5۔ سوشل انجینئرنگ اور اس کے اثرات

6۔ سائبر کیفے اور سائبر جرائم

7۔ سائبر کیفے میں سائبر جرائم کے ارتکاب کے طریقے

8۔ حقیقی دنیا کے سائبر کرائم کیسز

9۔ WannaCry Ransomware Attack

10۔ Yahoo Data Breach

11۔ قانونی فریم ورک اور سائبر کرائم قوانین

12۔ GDPR

13۔ CFAA

14۔ IT Act 2000

15۔ سائبر جرائم کے خلاف حفاظتی اقدامات

16۔ سائبر سیکیورٹی کے بہترین طریقے(Best Practices)

اکائی4۔ سائبر اسپیس اور قانون اور سائبر فورینسکس

(Cyberspace and the Law & Cyber Forensics)

اکائی کے اجزاء

4.0 تمہید

4.1 مقاصد

4.2 سائبر اسپیس

4.3 بین الاقوامی قوانین کا کردار

4.4 سائبر کرائم کے لیے بین الاقوامی قانون

4.5 تعارف: سائبر فارنزکس

4.6 ای میل کا فرانزک تجزیہ:

4.7 فارنسک ٹولز کو ای میل کریں۔

4.8 فرانزک تحقیقات(Forensics Investigation)

4.9 وسائل کے چیلنجز کی اقسام یہ ہیں:

4.10 اکتسابی نتائج

4.11 کلیدی الفاظ

4.12 نمونہ امتحانی سوالات

4.13 تجویز کردہ اکتسابی مواد

4.0 تمہید

سائبر اسپیس ایک پیچیدہ ماحول ہے جس میں لوگ، سافٹ ویئر اور مختلف خدمات ایک دوسرے کے ساتھ تعامل کرتے ہیں۔اس میں دنیا بھر میں پھیلے ہوئے معلوماتی اور مواصلاتی ٹیکنالوجی کے آلات اور نیٹ ورکس شامل ہوتے ہیں۔ سائبر اسپیس کے بڑھتے ہوئے استعمال کے ساتھ سائبر جرائم اور سائبر سیکیورٹی سے متعلق مسائل میں بھی اضافہ ہوا ہے۔

4.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- سائبر اسپیس کے بنیادی تصور کو سمجھ سکے گا۔
- سائبر اسپیس میں بین الاقوامی قوانین کے کردار کو بیان کر سکے گا۔
- سائبر کرائم سے متعلق بین الاقوامی قوانین کو سمجھ سکے گا۔
- سائبر فارنزکس کے بنیادی تصور کی وضاحت کر سکے گا۔
- ای میل کے فارنزک تجزیے کے مختلف طریقوں کو سمجھ سکے گا۔
- مختلف ای میل فارنزک ٹولز سے واقف ہو سکے گا۔
- فارنزک تحقیقات کے مراحل کو بیان کر سکے گا۔

4.2 سائبر اسپیس

سائبر اسپیس کو ایک پیچیدہ ماحول کے طور پر بیان کیا جاسکتا ہے جس میں لوگوں، سافٹ ویئر اور خدمات کے درمیان تعامل شامل ہوتا ہے۔ یہ معلومات اور مواصلاتی ٹیکنالوجی کے آلات اور نیٹ ورکس کی دنیا بھر میں تقسیم کے ذریعے برقرار رکھا جاتا ہے۔

تکنیکی ترقی سے حاصل ہونے والے فوائد کے ساتھ، سائبر اسپیس آج شہریوں، کاروباروں، اہم معلوماتی ڈھانچے، فوج اور حکومتوں کی طرف سے استعمال ہونے والا ایک عام پول بن گیا ہے جس کی وجہ سے ان مختلف گروہوں کے درمیان واضح حدود قائم کرنا مشکل ہو جاتا ہے۔ سائبر اسپیس (Cyberspace) کے آنے والے سالوں میں مزید پیچیدہ ہونے کی توقع ہے، اس سے منسلک نیٹ ورکس اور آلات میں اضافے کے ساتھ ہے۔

ضابطے (Regulations)

سائبر سیکیوریٹی کے حوالے سے پانچ اہم قوانین ہیں:-انفارمیشن ٹکنالوجی ایکٹ، 2000 ہندوستانی سائبر قوانین انفارمیشن ٹیکنالوجی ایکٹ کے زیر انتظام ہیں، جو 2000 میں لکھے گئے تھے۔ اس ایکٹ کا بنیادی محرک ای کامرس کو قابل اعتماد قانونی شمولیت کی پیشکش کرنا ہے، جو حکومت کے ساتھ حقیقی وقت کے ریکارڈ کے اندراج کی سہولت فراہم کرتا ہے۔

لیکن سائبر حملہ آوروں کے چپکے سے، ٹیکنالوجی کے غلط استعمال کے انسانی رجحان میں سر فہرست ہونے کے بعد، ترمیم کا ایک سلسلہ شروع ہوا۔

آئی ٹی اے، جسے ہندوستان کی پارلیمنٹ نے نافذ کیا ہے، ای گورننس، ای بینکنگ، اور ای کامرس کے شعبوں کے تحفظ کے لیے سنگین سزاؤں اور سزاؤں کو نمایاں کرتا ہے۔ اب، تمام جدید ترین مواصلاتی آلات کو شامل کرنے کے لیے ITA کے دائرہ کار کو بڑھا دیا گیا ہے۔

آئی ٹی ایکٹ نمایاں ہے، جو سائبر کرائمز پر سختی سے قابو پانے کے لیے پوری ہندوستانی قانون سازی کی رہنمائی کرتا ہے:

دفعہ 43-ان لوگوں پر لاگو ہوتا ہے جو مالک کی اجازت کے بغیر کمپیوٹر سسٹم کو نقصان پہنچاتے ہیں۔ مالک ایسے معاملات میں پورے نقصان کے معاوضے کا مکمل دعوی کر سکتا ہے۔

دفعہ 66-اس صورت میں لاگو ہوتا ہے جب کوئی شخص بے ایمانی یا دھوکہ دہی سے سیکشن 43 میں کسی بھی کام کا ارتکاب کرتا پایا جاتا ہے۔ 5 لاکھ

دفعہ 66B- چوری شدہ مواصلاتی آلات یا کمپیوٹرز کو دھوکہ دہی سے حاصل کرنے کی سزا کو شامل کرتا ہے، جو ممکنہ تین سال قید کی تصدیق کرتا ہے۔ یہ اصطلاح بھی روپے سے اوپر جا سکتی ہے۔ 1 لاکھ جرمانہ، شدت کے لحاظ سے۔

دفعہ 66C- یہ سیکشن جعلی ڈیجیٹل دستخطوں، ہیکنگ پاس ورڈز، یا دیگر مخصوص شناختی خصوصیات سے متعلق شناختی چوریوں کی جانچ پڑتال کرتا ہے۔ جرم ثابت ہونے پر تین سال قید کی سزا کے ساتھ ایک لاکھ روپے جرمانہ بھی ہو سکتا ہے۔ دفعہ 66D- یہ سیکشن آن ڈیمانڈ داخل کیا گیا تھا، جس میں کمپیوٹر وسائل کا استعمال کرتے ہوئے نقالی کرنے والے دھوکہ بازوں کو سزا دینے پر توجہ مرکوز کی گئی تھی۔

تعزیرات ہند 1980 Indian Panel Code (IPC)

شناختی چوری اور متعلقہ سائبر فراڈ انڈین پینل کوڈ 1860، (IPC) میں مجسم ہیں- 2000 کے انفارمیشن ٹیکنالوجی ایکٹ کے ساتھ درخواست کی گئی۔ IPC کا بنیادی متعلقہ سیکشن سائبر فراڈ کا احاطہ کرتا ہے:

جعلسازی (دفعہ 464)

دھوکہ دہی کے لیے پہلے سے منصوبہ بندی کی گئی جعلسازی (دفعہ 468) غلط دستاویزات (دفعہ 465)

جعلی دستاویز کو حقیقی کے طور پر پیش کرنا (سیکشن 471) ساکھ کو نقصان پہنچانا (سیکشن 469)

کمپنیز ایکٹ 2013

کارپوریٹ اسٹیک ہولڈرز کمپنیز ایکٹ 2013 کو روزمرہ کے کاموں کی اصلاح کے لیے ضروری قانونی ذمہ داری کے طور پر حوالہ دیتے ہیں۔ اس ایکٹ کی ہدایات تمام مطلوبہ تکنیکی قانونی تعمیل کو مستحکم کرتی ہیں، جس سے کم تعمیل کرنے والی کمپنیوں کو قانونی طور پر حل کیا جاتا ہے۔

کمپنیز ایکٹ 2013 نے SFIO (Serious Frauds Investigation Office) کو ہندوستانی کمپنیوں اور ان کے ڈائریکٹرز پر مقدمہ چلانے کے اختیارات سونپے ہیں۔ نیز، کمپنیز انسپیکشن، انویسٹمنٹ اور انکوائری رولز، 2014 کے نوٹیفکیشن کے بعد، SFIOs اس سلسلے میں اور زیادہ فعال اور سخت ہو گئے ہیں۔

مقننہ (legislature) نے اس بات کو یقینی بنایا کہ تمام ریگولیٹری تعمیل کو اچھی طرح سے احاطہ کیا گیا ہے، بشمول سائبر فرانزک، ای ڈسکوری، اور سائبر سیکیورٹی (Cyber security) ڈیلیجنس۔ کمپنیز (مینجمنٹ اینڈ ایڈمنسٹریشن) رولز، 2014 کمپنی کے ڈائریکٹرز اور لیڈروں پر سائبر سیکیورٹی (Cyber security) کی ذمہ داریوں اور ذمہ داریوں کی تصدیق کرنے والے سخت رہنما خطوط

تجویز کرتا ہے۔

NIST Compliance تعمیل

سائبر سیکیوریٹی فریم ورک (NCFS)، جسے نیشنل انسٹی ٹیوٹ آف اسٹینڈرڈز اینڈ ٹیکنالوجی (NIST) نے اختیار کیا ہے، سب سے زیادہ قابل اعتماد عالمی سرٹیفائینگ باڈی کے طور پر سائبر سیکیوریٹی کے لیے ایک ہم آہنگ طریقہ پیش کرتا ہے۔

NIST سائبر سیکیوریٹی فریم ورک سائبر سے متعلقہ خطرات کو ذمہ داری کے ساتھ منظم کرنے کے لیے تمام مطلوبہ رہنما خطوط، معیارات اور بہترین طریقوں پر مشتمل ہے۔اس فریم ورک کو لچک اور لاگت کی تاثیر پر ترجیح دی جاتی ہے۔

یہ اہم بنیادی ڈھانچے کی لچک اور تحفظ کو فروغ دیتا ہے بذریعہ: سائبر سیکیوریٹی خطرات کی بہتر تشریح، انتظام، اور کمی کی اجازت دے کر—ڈیٹا کے نقصان، ڈیٹا کے غلط استعمال، اور اس کے نتیجے میں بحالی کے اخراجات کو کم کرنے کے لیے اہم ترین سرگرمیوں اور اہم کارروائیوں کا تعین کرنا—ان کو محفوظ بنانے پر توجہ مرکوز کرنا اہم اثاثوں کو محفوظ کرنے والی تنظیموں کے اعتماد کی اہلیت کو ظاہر کرتا ہے۔ سائبر سیکیوریٹی ROI کو زیادہ سے زیادہ بنانے کے لیے سرمایہ کاری کو ترجیح دیں ریگولیٹری اور معاہدہ کی ذمہ داریوں کو ایڈریس کرتا ہے وسیع تر انفارمیشن سیکیورٹی پروگرام کی حمایت کرتا ہے NIST CSF فریم ورک کو ISO/IEC 27001 کے ساتھ ملا کر - سائبر سیکیورٹی (Cyber security) رسک مینجمنٹ کو آسان بنایا جاتا ہے۔ یہ مواصلات کو بھی آسان بناتا ہے۔

NIST کی طرف سے وضع کردہ ایک مشترکہ سائبر سیکیوریٹی ہدایت کے ذریعے پوری تنظیم اور سپلائی چینز میں۔

حتمی خیالات جیسے جیسے ٹیکنالوجی پر انسانی انحصار تیز ہوتا جارہا ہے، ہندوستان اور پوری دنیا میں سائبر قوانین کو مسلسل اپ گریڈیشن اور اصلاح کی ضرورت ہے۔ وبائی مرض نے بھی زیادہ تر افرادی قوت کو دور دراز کے کام کرنے والے ماڈیول میں دھکیل دیا ہے جس سے ایپ سیکیورٹی کی ضرورت میں اضافہ ہوتا ہے۔ قانون سازوں کو دھوکے بازوں سے آگے رہنے کے لیے اضافی میل طے کرنا پڑتا ہے، تاکہ ان کی آمد پر انہیں روکا جاسکے۔

سائبر کرائمز کو کنٹرول کیا جاسکتا ہے لیکن اس کے لیے قانون سازوں، انٹرنیٹ یا نیٹ ورک فراہم کرنے والوں، بینکوں اور شاپنگ سائٹس جیسے سفارشی، اور سب سے اہم، صارفین کی مشترکہ کوششوں کی ضرورت ہے۔ سائبر لینڈ کے قانون میں ان کی قید کو یقینی بناتے ہوئے ان اسٹیک ہولڈرز کی صرف دانشمندانہ کوششیں ہی آن لائن حفاظت اور لچک پیدا کرسکتی ہیں۔

4.3 بین الاقوامی قوانین کا کردار

مختلف ممالک میں کمپیوٹنگ اور کمیونیکیشن انڈسٹریز کے شعبوں کو حکومتی اداروں کے ذریعے کنٹرول کیا جاتا ہے۔ کمپیوٹرز اور کمپیوٹر نیٹ ورکس کے استعمال کے بارے میں مخصوص اصول ہیں، خاص طور پر غیر مجاز رسائی، ڈیٹا پرائیویسی اور سپیمنگ کے اصول ہیں۔ خفیہ کاری اور آلات کے استعمال پر بھی حدود ہیں جو کاپی پروٹیکشن اسکیموں کو شکست دینے کے لیے استعمال کیے جاسکتے ہیں۔1انٹرنیٹ پر تجارت، ٹیکس لگانے، صارفین کے تحفظ اور اشتہارات کو کنٹرول کرنے والے قوانین موجود ہیں۔ سنسر شپ (sensership) بمقابلہ اظہار رائے کی

آزادی، سرکاری معلومات تک عوامی رسائی کے قوانین، اور نجی اداروں کے ذریعہ ان پر رکھی گئی معلومات تک انفرادی رسائی کے قوانین موجود ہیں۔1کچھ ریاستیں قانون کے ساتھ ساتھ تکنیکی ذرائع سے انٹرنیٹ تک رسائی کو محدود کرتی ہیں۔

4.4 سائبر کرائم کے لیے بین الاقوامی قانون

سائبر کرائم "بین الاقوامی" ہے کہ 'ممالک کے درمیان سائبر بارڈرز نہیں ہیں'1سائبر کرائم کی اقسام اور شکلوں میں پیچیدگی اس سے لڑنے میں دشواری کو بڑھاتی ہے۔ سائبر کرائم کے خلاف جنگ بین الاقوامی تعاون کی ضرورت ہے۔1مختلف تنظیموں اور حکومتوں نے پہلے ہی علاقائی اور بین الاقوامی سطح پر قانون سازی اور قانون کے نفاذ کے عالمی معیارات قائم کرنے کے لیے مشترکہ کوششیں کی ہیں۔

ہندوستانی سائبر اسپیس

ہندوستانی سائبر اسپیس 1975 میں نیشنل انفارمیٹکس سینٹر (NIC) کے قیام کے ساتھ پیدا ہوا تھا جس کا مقصد حکومت کو IT حل فراہم کرنا تھا۔ حکومت کی مختلف ایجنسیوں کو جوڑنے کے لیے 1986 اور 1988 کے درمیان تین نیٹ ورک (NWs) قائم کیے گئے۔ یہ NWs تھے، INDONET جس نے IBM مین فریم تنصیبات کو جوڑ دیا جس نے ہندوستان کا کمپیوٹر انفراسٹرکچر بنایا، NICNET (NIC NW) پبلک سیکٹر کی تنظیموں کے ساتھ ساتھ مرکزی حکومت کو ریاستی حکومتوں سے جوڑنے کے لیے ایک ملک گیر بہت چھوٹا اپرچر ٹرمینل NW (VSAT)۔اور ضلعی انتظامیہ، تیسرا NW سیٹ اپ ERNET (تعلیمی اور تحقیقی نیٹ ورک) تھا، تاکہ تعلیمی اور تحقیق کی خدمت کی جاسکے۔ کمیونٹیز:1998 کی نئی انٹرنیٹ پالیسی نے متعدد انٹرنیٹ سروس پرووائیڈرز (ISPs) کی خدمات کے لیے راہ ہموار کی اور انٹرنیٹ صارفین کی تعداد کو بڑھایا جو 1999 میں 1.4 ملین سے بڑھ کر دسمبر 2012 تک 150 ملین سے زیادہ ہو گیا۔ موبائل فون اور گولیاں. حکومت براڈ بینڈ کو بڑھانے کے لیے پر عزم ہے۔ تقریباً6%1 کی موجودہ سطح سے دخول۔ نیشنل براڈ بینڈ پلان کے تحت2016تک براڈ بینڈ کا ہدف160 ملین گھرانوں کا ہے۔

نیشنل سائبر سیکیورٹی(Cyber security)پالیسی

نیشنل سائبر سیکیورٹی(Cyber security)پالیسی ایک پالیسی فریم ورک ہے جس کے ذریعے محکمہ الیکٹرانکس اور انفارمیشن ٹیکنالوجی اس کا مقصد پبلک اور پرائیویٹ انفراسٹرکچر کو سائبر حملوں سے بچانا ہے۔ پالیسی "معلومات، جیسے ذاتی معلومات (ویب صارفین کی)، مالیاتی اور بینکنگ کی معلومات اور خود مختار ڈیٹا" کی حفاظت کا ارادہ رکھتی ہے۔ کے تناظر میں یہ خاص طور پر متعلقہ تھا امریکی قومی سلامتی ایجنسی (NSA) لیکس جس نے تجویز کیا کہ امریکی حکومتی ایجنسیاں ہندوستانی صارفین کی جاسوسی کر رہی ہیں، جن کے خلاف کوئی قانونی یا تکنیکی تحفظات نہیں ہیں۔ وزارت مواصلات اور انفارمیشن ٹیکنالوجی (بھارت) وضاحت کرتا ہے سائبر اسپیس ایک پیچیدہ ماحول کے طور پر جو لوگوں کے درمیان تعاملات پر مشتمل ہے، معلومات اور مواصلاتی ٹیکنالوجی کی دنیا بھر میں تقسیم کے ذریعے تعاون یافتہ سافٹ ویئر سروسز۔

ویژن: شہریوں، کاروبار اور حکومت کے لیے ایک محفوظ اور لچکدار سائبر اسپیس بنانے کے لیے اور کسی کو بھی صارف کی رازداری میں مداخلت سے بچانے کے لیے۔

مشن: سائبر اسپیس میں معلومات اور انفارمیشن انفراسٹرکچر کی حفاظت کے لیے، سائبر خطرے کو روکنے اور اس کا جواب دینے کے لیے صلاحیتیں پیدا کرنا، کمزوریوں کو کم کرنا اور ادارہ جاتی ڈھانچے، لوگوں، عمل، ٹیکنالوجی، اور تعاون کے امتزاج کے ذریعے سائبر واقعات سے ہونے والے نقصان کو کم کرنا۔

مقصد:

وزارت مواصلات اور انفارمیشن ٹیکنالوجی (بھارت) مندرجہ ذیل مقاصد کی وضاحت کریں:

- ملک میں ایک محفوظ سائبر ماحولیاتی نظام کی تشکیل کے لیے، آئی ٹی سسٹم اور سائبر اسپیس میں لین دین میں خاطر خواہ اعتماد اور اعتماد پیدا کریں اور اس طرح معیشت کے تمام شعبوں میں آئی ٹی کو اپنانے میں اضافہ کریں۔
- حفاظتی پالیسیوں کے ڈیزائن اور فروغ کے لیے ایک یقین دہانی کا فریم ورک بنانا اور عالمی سلامتی کے معیارات کی تعمیل کے لیے اقدامات کو فعال کرنا اور ہم آہنگی کی تشخیص (مصنوعات، عمل، ٹیکنالوجی اور افراد) کے ذریعے بہترین طرز عمل۔
- ایک محفوظ سائبر اسپیس ماحولیاتی نظام کو یقینی بنانے کے لیے ریگولیٹری فریم ورک کو مضبوط کرنا۔
- آئی سی ٹی کے بنیادی ڈھانچے کو درپیش خطرات کے بارے میں حکمت عملی کی معلومات حاصل کرنے کے لیے قومی اور سیکٹرل سطح کے 24X7 میکانزم کو بڑھانا اور بنانا، مؤثر پیشن گوئی، حفاظتی، حفاظتی ردعمل اور بحالی کے اقدامات کے ذریعے ردعمل، حل اور بحران کے انتظام کے لیے منظر نامے تیار کرنا۔

4.5 تعارف: سائبر فارنزکس

سائبر فارنزکس: کمپیوٹر فرانزک ثبوت جمع کرنے اور محفوظ کرنے کے لیے تفتیش اور تجزیہ کی تکنیک کا استعمال ہے۔

فرانزک ایگزامینرز عام طور پر پرسنل کمپیوٹرز، لیپ ٹاپس، پرسنل ڈیجیٹل اسسٹنٹس، سیل فونز، سرورز، ٹیپس اور کسی دوسرے قسم کے میڈیا سے ڈیٹا کا تجزیہ کرتے ہیں۔ اس عمل میں بریکنگ انکرپشن، قانون نافذ کرنے والی ٹیم کے ساتھ سرچ وارنٹ پر عمل درآمد، ہارڈ ڈرائیوز سے فائلوں کی بازیافت اور تجزیہ کرنے تک کچھ بھی شامل ہو سکتا ہے جو انتہائی سنگین سول اور فوجداری مقدمات میں اہم ثبوت ہوں گے۔

کمپیوٹرز اور ڈیٹا سٹوریج میڈیا کا فرانزک معائنہ ایک پیچیدہ اور انتہائی خصوصی عمل ہے۔ فرانزک امتحانات کے نتائج مرتب کیے جاتے ہیں اور رپورٹس میں شامل کیے جاتے ہیں۔ بہت سے معاملات میں، ممتحن اپنے نتائج کی گواہی دیتے ہیں، جہاں ان کی مہارت اور قابلیت کو حتمی جانچ پڑتال کے لیے رکھا جاتا ہے۔

ڈیجیٹل فارنسک: ڈیجیٹل فرانزکس کی تعریف کمپیوٹر شواہد کو محفوظ کرنے، شناخت کرنے، نکالنے اور دستاویزات بنانے کے عمل کے طور پر کی گئی ہے جسے عدالت کے ذریعے استعمال کیا جا سکتا ہے۔ یہ ڈیجیٹل میڈیا جیسے کمپیوٹر، موبائل فون، سرور، یا نیٹ ورک سے ثبوت تلاش کرنے کی سائنس ہے۔ یہ فرانزک ٹیم کو ڈیجیٹل سے متعلق پیچیدہ معاملات کو حل کرنے کے لیے بہترین تکنیک اور اوزار فراہم کرتا ہے۔

ڈیجیٹل فرانزک فرانزک ٹیم کو مختلف قسم کے الیکٹرانک آلات پر موجود ڈیجیٹل شواہد کا تجزیہ، معائنہ، شناخت اور محفوظ کرنے میں مدد کرتا ہے۔

ڈیجیٹل فرانزک سائنس فرانزک سائنس کی ایک شاخ ہے جو سائبر کرائم سے متعلق ڈیجیٹل آلات میں پائے جانے والے مواد کی بازیابی اور تفتیش پر مرکوز ہے۔

کمپیوٹر فارنسک کی ضرورت

کمپیوٹر فرانزک بھی اہم ہے کیونکہ اس سے آپ کی تنظیم کے پیسے بچ سکتے ہیں۔ سے a

تکنیکی نقطہ نظر سے، کمپیوٹر فرانزک کا بنیادی مقصد ڈیٹا کی شناخت، جمع، محفوظ اور تجزیہ کرنا ہے تاکہ جمع کیے گئے شواہد کی سالمیت کو محفوظ رکھا جاسکے تاکہ اسے قانونی کیس میں مؤثر طریقے سے استعمال کیا جاسکے۔

سائبر فارنزکس اور ڈیجیٹل ثبوت: ڈیجیٹل ثبوت وہ معلومات ہیں جو بائنری شکل میں محفوظ یا منتقل کی جاتی ہیں جن پر عدالت میں بھروسہ کیا جا سکتا ہے۔ یہ کمپیوٹر ہارڈ ڈرائیو، موبائل فون، اور دیگر جگہوں پر پایا جاسکتا ہے۔ ڈیجیٹل ثبوت عام طور پر الیکٹرانک کرائم، یا ای کرائم، جیسے چائلڈ پورنوگرافی یا کریڈٹ کارڈ فراڈ سے منسلک ہوتے ہیں۔ تاہم، ڈیجیٹل ثبوت اب صرف ای کرائم ہی نہیں بلکہ تمام قسم کے جرائم پر مقدمہ چلانے کے لیے استعمال کیے جاتے ہیں۔ مثال کے طور پر، مشتبہ افراد کی ای میل یا موبائل فون فائلوں میں ان کے ارادے، جرم کے وقت ان کے ٹھکانے اور دوسرے مشتبہ افراد کے ساتھ ان کے تعلقات کے بارے میں اہم ثبوت ہو سکتے ہیں۔ مثال کے طور پر 2005 میں، ایک فلاپی ڈسک نے تفتیش کاروں کو BTK سیریل کلر تک پہنچایا جو 1974 سے پولیس کی گرفتاری سے بچ گیا تھا اور کم از کم 10 متاثرین کی جانیں لے چکا تھا۔

ای کرائم سے لڑنے اور تمام جرائم کے لیے متعلقہ ڈیجیٹل شواہد اکٹھا کرنے کی کوشش میں، قانون نافذ کرنے والی ایجنسیاں ڈیجیٹل شواہد، جسے کمپیوٹر فرانزک بھی کہا جاتا ہے، کو اپنے انفراسٹرکچر میں شامل کر رہے ہیں۔ قانون نافذ کرنے والے اداروں کو افسران کو ڈیجیٹل شواہد اکٹھا کرنے اور کمپیوٹر آپریٹنگ سسٹم جیسی تیزی سے ترقی پذیر ٹیکنالوجیز کے ساتھ چلنے کی تربیت دینے کی ضرورت کا سامنا ہے۔

4.6 ای میل کا فرانزک تجزیہ

ای میل فرانزک سے مراد ای میل کے ماخذ اور مواد کا مطالعہ بطور ثبوت ہے جس سے پیغام کے اصل بھیجنے والے اور وصول کنندہ کی شناخت، ڈیٹا/ٹرانسمیشن کا وقت، ای میل لین دین کا تفصیلی ریکارڈ، بھیجنے والے کا ارادہ وغیرہ۔ اس مطالعہ میں تصنیف کے انتساب اور ای میل گھوٹالوں کی شناخت کے لیے میٹاڈیٹا، مطلوبہ الفاظ کی تلاش، پورٹ اسکیننگ وغیرہ کی تحقیقات شامل ہیں۔

ای میل فرانزک کے لیے مختلف طریقے استعمال کیے جاتے ہیں:

ہیڈر تجزیہ - کنٹرول معلومات کی شکل میں ای میل پیغام میں میٹاڈیٹا

یعنی لفافہ اور ہیڈر بشمول میسج باڈی میں ہیڈر بھیجنے والے اور/یا اس راستے کے بارے میں معلومات پر مشتمل ہوتا ہے جس سے پیغام گزرا ہے۔

ان میں سے کچھ کو بھیجنے والے کی شناخت چھپانے کے لیے جعل سازی کی جاسکتی ہے۔ان ہیڈرز اور ان کے باہمی تعلق کا تفصیلی تجزیہ ہیڈر تجزیہ میں کیا جاتا ہے۔

بیت کی حکمت عملی-بیت بازی کے حربے کی تفتیش میں ایک ای میل جس میں imgsrc>" :http>"ٹیگ ہے جس میں تفتیش کاروں کے زیر نگرانی کچھ کمپیوٹر پر تصویری ماخذ موجود ہے جو تفتیش کے تحت ای میل بھیجنے والے کو بھیج دیا جاتا ہے جس میں اصلی (حقیقی) ای میل پتہ ہوتا ہے۔جب ای میل کھولی جاتی ہے تو، ایک لاگ انٹری جس میں وصول کنندہ کا IP ایڈریس ہوتا ہے (تفتیش کے تحت ای میل بھیجنے والا) تصویر کی میزبانی کرنے والے HTTP سرور پر ریکارڈ کیا جاتا ہے اور اس طرح بھیجنے والے کو ٹریک کیا جاتا ہے۔تاہم، اگر وصول کنندہ (تفتیش کے تحت ای میل بھیجنے والا) پراکسی سرور استعمال کر رہا ہے تو پراکسی سرور کا آئی پی ایڈریس ریکارڈ کیا جاتا ہے۔لاگ آن پراکسی سرور کو زیر تفتیش ای میل بھیجنے والے کو ٹریک کرنے کے لیے استعمال کیا جاسکتا ہے۔اگر پراکسی سرور کا لاگ کسی وجہ سے دستیاب نہیں ہے، تو تفتیش کار ایک ٹیکٹ ای میل بھیج سکتے ہیں جس میں ایک)ایمبیڈڈ جاوا ایپلٹ جو ریسیور کے کمپیوٹر پر چلتا ہے یا ب)ایکٹو ایکس آبجیکٹ کے ساتھ ایچ ٹی ایم ایل صفحہ۔دونوں کا مقصد وصول کنندہ کے کمپیوٹر کا آئی پی ایڈریس نکالنا اور اسے تفتیش کاروں کو ای میل کرنا ہے۔

سرور کی تحقیقات—اس تفتیش میں، ای میل پیغام کے ماخذ کی شناخت کے لیے ڈیلیور کی گئی ای میلز اور سرور لاگز کی چھان بین کی جاتی ہے۔ کلائنٹس (بھیجنے والے یا وصول کنندگان) سے صاف کیے گئے ای میلز جن کی بازیابی ناممکن ہے سرورز (پراکسی یا آئی ایس پی) سے درخواست کی جاسکتی ہے کیونکہ ان میں سے زیادہ تر اپنی ڈیلیوری کے بعد تمام ای میلز کی کاپی اسٹور کرتے ہیں۔مزید برآں، سرورز کے ذریعے رکھے گئے لاگز کا مطالعہ کیا جاسکتا ہے تاکہ ای میل لین دین کرنے کے لیے ذمہ دار کمپیوٹر کا پتہ معلوم کیا جاسکے۔تاہم، سرورز ای میل اور سرور لاگز کی کاپیاں صرف کچھ محدود مدت کے لیے اسٹور کرتے ہیں اور کچھ تفتیش کاروں کے ساتھ تعاون نہیں کر سکتے ہیں۔اس کے علاوہ، SMTP سرور جو ڈیٹا کو ذخیرہ کرتے ہیں جیسے کریڈٹ کارڈ نمبر اور میل باکس کے مالک سے متعلق دیگر ڈیٹا کو ای میل ایڈریس کے پیچھے موجود شخص کی شناخت کے لیے استعمال کیا جاسکتا ہے۔

نیٹ ورک ڈیوائس کی تفتیش—ای میل کی تفتیش کی اس شکل میں، نیٹ ورک ڈیوائسز جیسے کہ روٹرز، فائر والز اور سوئچز کے ذریعے رکھے گئے لاگز کو ای میل پیغام کے ماخذ کی چھان بین کے لیے استعمال کیا جاتا ہے۔تفتیش کی یہ شکل پیچیدہ ہے اور صرف اس وقت استعمال ہوتی ہے جب سرورز کے لاگز (Proxy یا ISP) کسی وجہ سے دستیاب نہ ہوں، جیسے جب ISP یا پراکسی لاگ کو برقرار نہیں رکھتا ہے یا ISP کی طرف سے تعاون کی کمی ہے یا ثبوت کا سلسلہ برقرار رکھنے میں ناکام ہے۔

سافٹ ویئر ایمبیڈڈ شناخت کنندگان-ای میل کے تخلیق کار کے بارے میں کچھ معلومات، منسلک فائلوں یا دستاویزات کو ای میل سافٹ ویئر کے ذریعے پیغام کے ساتھ شامل کیا جاسکتا ہے۔

بھیجنے والے کے ذریعہ ای میل تحریر کرنے کے لیے استعمال کیا جاتا ہے۔یہ معلومات اپنی مرضی کے ہیڈر کی شکل میں یا MIME مواد کی شکل میں ٹرانسپورٹ نیوٹرل انکیپسولیشن فارمیٹ (TNEF) کے طور پر شامل کی جاسکتی ہے۔ان تفصیلات کے لیے ای میل کی چھان بین کرنے سے ای میل بھیجنے والوں کی ترجیحات اور اختیارات کے بارے میں کچھ اہم معلومات سامنے آسکتی ہیں جو کلائنٹ کی طرف سے ثبوت

جمع کرنے میں مدد کر سکتی ہیں۔ تحقیقات سے ای میل پیغام بھیجنے کے لیے استعمال ہونے والے کلائنٹ کمپیوٹر کے PST فائل کے نام، ونڈوز لاگ ان صارف نام، میک ایڈریس وغیرہ کا پتہ چل سکتا ہے۔

بھیجنے والے میلر کے فنگر پرنٹس - سرور پر سافٹ ویئر ہینڈلنگ ای میل کی شناخت موصول شدہ ہیڈر فیلڈ سے ظاہر کی جاسکتی ہے اور کلائنٹ پر سافٹ ویئر ہینڈلنگ ای میل کی شناخت مختلف ہیڈرز جیسے "X-Mailer" یا اس کے مساوی استعمال کر کے معلوم کی جاسکتی ہے۔ یہ ہیڈرز ای میل بھیجنے کے لیے کلائنٹس پر استعمال ہونے والی ایپلیکیشنز اور ان کے ورژن کی وضاحت کرتے ہیں۔ بھیجنے والے کے کلائنٹ کمپیوٹر کے بارے میں یہ معلومات تفتیش کاروں کو ایک موثر منصوبہ تیار کرنے میں مدد کے لیے استعمال کی جاسکتی ہیں اور اس طرح یہ بہت مفید ثابت ہوتی ہے۔

4.7 فارنسک ٹولز کو ای میل کریں

کسی ای میل کو مٹانے یا حذف کرنے کا لازمی طور پر یہ مطلب نہیں ہے کہ وہ ہمیشہ کے لیے ختم ہو گئی ہے۔ اکثر ای میلز کو ڈیلیٹ کرنے کے بعد بھی فرانزک طور پر نکالا جاسکتا ہے۔ ای میل کی فرانزک ٹریسنگ روایتی جاسوسی کام کی طرح ہے۔ یہ میل باکس فائلوں سے معلومات کی بازیافت کے لیے استعمال ہوتا ہے۔

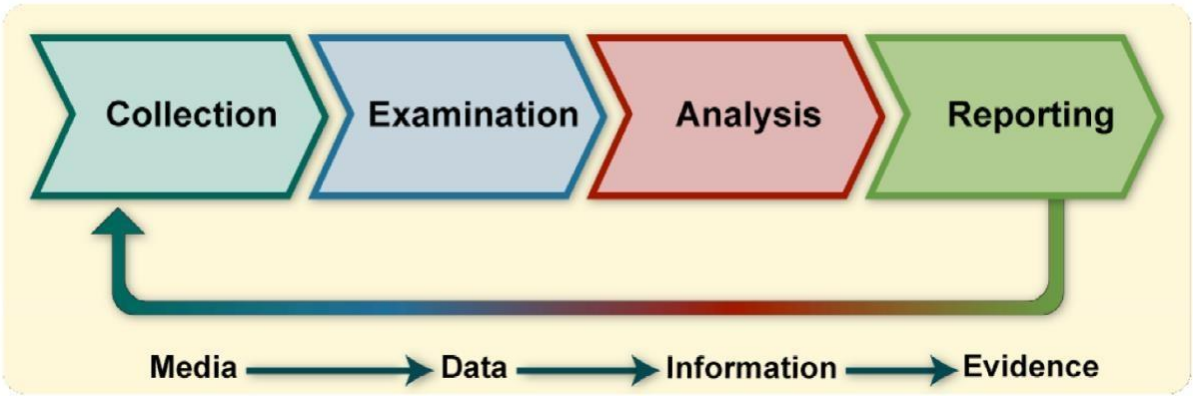
MiTec میل ناظر - یہ آؤٹ لک ایکسپریس، ونڈوز میل/ونڈوز لائیو میل، موزیلا تھنڈر برڈ میسج ڈیٹا بیس، اور واحد EML فائلوں کا ناظر ہے۔ یہ تمام ضروری خصوصیات کے ساتھ موجود پیغامات کی فہرست دکھاتا ہے، جیسے ایک عام ای میل کلائنٹ۔ پیغامات کو تفصیلی منظر میں دیکھا جاسکتا ہے، بشمول منسلکات اور ایچ ٹی ایم ایل پیش نظارہ۔ اس میں طاقتور تلاش اور فلٹرنگ کی صلاحیت ہے اور یہ کھلے ہوئے فولڈر میں موجود تمام ای میلز سے ای میل پتوں کو ایک کلک کے ذریعے فہرست میں نکالنے کی بھی اجازت دیتا ہے۔ منتخب پیغامات کو ایم ایل فائلوں میں ان کے منسلکات کے ساتھ یا اس کے بغیر محفوظ کیا جاسکتا ہے۔ منسلکات کو منتخب پیغامات سے ایک کمانڈ کے ذریعے نکالا جاسکتا ہے۔

OST اور PST ناظر - نیو کلئس ٹیکنالوجیز کے OST اور PST ویور ٹولز آپ کو MS ایکسچینج سرور سے منسلک کیے بغیر آسانی سے OST اور PST فائلوں کو دیکھنے میں مدد کرتے ہیں۔ یہ ٹولز صارف کو OST اور PST فائلوں کو اسکین کرنے کی اجازت دیتے ہیں اور وہ اس میں محفوظ کردہ ڈیٹا بشمول ای میل پیغامات، روابط، کیلنڈرز، نوٹس وغیرہ کو فولڈر کے مناسب ڈھانچے میں دکھاتے ہیں۔

eMailTrackerPro - emailTrackerPro ای میل کے ہیڈرز کا تجزیہ کرتا ہے تاکہ اس مشین کے IP ایڈریس کا پتہ لگایا جاسکے جس نے پیغام بھیجا تھا تاکہ بھیجنے والے کو ٹریک کیا جاسکے۔ یہ ایک ہی وقت میں متعدد ای میلز کو ٹریس کر سکتا ہے اور آسانی سے ان پر نظر رکھ سکتا ہے۔ آئی پی ایڈریس کا جغرافیائی محل وقوع خطرے کی سطح یا ای میل پیغام کی درستگی کا تعین کرنے کے لیے کلیدی معلومات ہے۔

ای میل ٹریسر - ای میل ٹریسر سائبر فرانزکس میں ریسورس سینٹر فار سائبر فارنکس (RCCF) کی ایک ہندوستانی کوشش ہے جو ہندوستان میں سائبر فرانزک کا ایک اہم مرکز ہے۔ یہ قانون نافذ کرنے والے اداروں کی ضروریات پر مبنی سائبر فرانزک ٹولز تیار کرتا ہے۔

ڈیجیٹل فرانزکس لائف سائیکل:



مجموعہ: فرانزک عمل کا پہلا مرحلہ ڈیٹا کے ممکنہ ذرائع کی نشاندہی کرنا اور ان سے ڈیٹا حاصل کرنا ہے۔

امتحان: ڈیٹا اکٹھا کرنے کے بعد، اگلا مرحلہ ڈیٹا کی جانچ کرنا ہے، جس میں جمع کردہ ڈیٹا سے معلومات کے متعلقہ ٹکڑوں کا اندازہ لگانا اور نکالنا شامل ہے۔ اس مرحلے میں OS یا ایپلیکیشن کی خصوصیات کو نظرانداز یا کم کرنا بھی شامل ہو سکتا ہے جو ڈیٹا اور کوڈ کو غیر واضح کرتی ہیں، جیسے کہ ڈیٹا کمپریشن، انکرپشن، اور ایکسیس کنٹرول میکانزم۔

تجزیہ: ایک بار متعلقہ معلومات نکالنے کے بعد، تجزیہ کار کو اس سے نتائج اخذ کرنے کے لیے ڈیٹا کا مطالعہ اور تجزیہ کرنا چاہیے۔ فرانزک کی بنیاد دستیاب اعداد و شمار کی بنیاد پر مناسب نتائج پر پہنچنے کے لیے یا اس بات کا تعین کرنے کے لیے کہ ابھی تک کوئی نتیجہ اخذ نہیں کیا جا سکتا ایک طریقہ کار کا استعمال کر رہا ہے۔

رپورٹنگ: تجزیہ کے مرحلے کے نتیجے میں معلومات کی تیاری اور پیش کرنے کا عمل۔ بہت سے عوامل رپورٹنگ کو متاثر کرتے ہیں، جن میں درج ذیل شامل ہیں:

1۔ متبادل وضاحتیں: جب کسی واقعہ کے بارے میں معلومات نامکمل ہوں، تو جو ہوا اس کی قطعی وضاحت تک پہنچنا ممکن نہیں۔ جب کسی واقعہ کی دو یا دو سے زیادہ قابل فہم وضاحتیں ہوتی ہیں، تو رپورٹنگ کے عمل میں ہر ایک پر مناسب غور کیا جانا چاہیے۔ تجزیہ کاروں کو تجویز کردہ ہر ممکنہ وضاحت کو ثابت یا غلط ثابت کرنے کی کوشش کرنے کے لیے ایک طریقہ کار کا استعمال کرنا چاہیے۔

2۔ سامعین کا خیال۔ سامعین کو جاننا جن کو ڈیٹا یا معلومات دکھائی جائیں گی ضروری ہے۔

3۔ قابل عمل معلومات۔ رپورٹنگ میں ڈیٹا سے حاصل کردہ قابل عمل معلومات کی نشاندہی بھی شامل ہے جو تجزیہ کار کو معلومات کے نئے ذرائع جمع کرنے کی اجازت دے سکتی ہے۔

4.8 فرانزک تحقیقات (Forensics Investigation)

فرانزک وہ سائنسی طریقے ہیں جو کسی جرم کو حل کرنے کے لیے استعمال ہوتے ہیں۔ فرانزک تفتیش ایک مشتبہ شخص کے بارے

میں کسی نتیجے پر پہنچنے کے لیے جرم سے متعلق تمام جسمانی شواہد کو اکٹھا کرنا اور تجزیہ کرنا ہے۔ تفتیش کار خون، سیال، یا فنگر پرنٹس، باقیات، ہارڈ ڈرائیوز، کمپیوٹرز، یا دیگر ٹیکنالوجی کو دیکھیں گے تاکہ یہ معلوم کیا جا سکے کہ جرم کیسے ہوا ہے۔ یہ ایک عمومی تعریف ہے، اگرچہ، چونکہ فارنزک کی متعدد اقسام ہیں۔

فرانزک تحقیقات کی اقسام

فرانزک اکاؤنٹنگ/آڈٹینگ

کمپیوٹر یا سائبر فرانزک

کرائم سین فرانزک

فرانزک آثار قدیمہ

فرانزک دندان سازی۔

فرانزک اینٹومولوجی

فرانزک گرافولوجی

فرانزک پیتھالوجی

فرانزک سائیکالوجی

فرانزک سائنس

فرانزک ٹاکسیولوجی

کمپیوٹر فارنزکس میں چیلنجز

ڈیجیٹل فرانزک کو مجرمانہ پائے جانے والے واقعات کی تعمیر نو میں سہولت فراہم کرنے کے لیے ڈیجیٹل ذرائع سے اخذ کردہ ڈیجیٹل شواہد کی شناخت، جمع کرنے، محفوظ کرنے، توثیق، تجزیہ، تشریح، اور پیش کرنے کے لیے سائنسی طور پر اخذ کردہ اور ثابت شدہ طریقوں کے استعمال کے طور پر بیان کیا گیا ہے۔ عملی نفاذ کے وقت ڈیجیٹل فرانزک تحقیقاتی طریقوں کو کچھ بڑے چیلنجوں کا سامنا کرنا پڑتا ہے۔ فہدی، کلارک اور فرنل کے مطابق ڈیجیٹل فرانزک چیلنجز کو تین بڑے سروں میں درجہ بندی کیا گیا ہے:

تکنیکی چیلنجز

قانونی چیلنجز

وسائل کے چیلنجز

تکنیکی چیلنجز

جیسے جیسے ٹیکنالوجی ترقی کرتی ہے جرائم اور مجرم بھی اس سے ترقی کرتے ہیں۔ ڈیجیٹل فرانزک ماہرین مجرموں کے خلاف شواہد

کے ٹکڑوں کو اکٹھا کرنے کے لیے فرانزک ٹولز کا استعمال کرتے ہیں اور مجرم اپنے جرم کے نشانات کو چھپانے، بدلنے یا ہٹانے کے لیے ایسے آلات کا استعمال کرتے ہیں، ڈیجیٹل فرانزک میں اس عمل کو اینٹی فارنزک تکنیک کہا جاتا ہے جسے ڈیجیٹل میں ایک بڑا چیلنج سمجھا جاتا ہے۔ فرانزک دنیا.

اینٹی فرانزک تکنیک کو درجہ ذیل اقسام میں تقسیم کیا جاتا ہے:

S. N.	قسم	تفصیل
1	خفیہ کاری	یہ قانونی طور پر معلومات کی رازداری کو یقینی بنانے کے لیے استعمال کیا جاتا ہے اسے کسی غیر مجاز صارف/ شخص سے پوشیدہ رکھ کر۔ بد قسمتی سے، یہ بھی کر سکتا ہے مجرم اپنے جرائم کو چھپانے کے لیے استعمال کرتے ہیں۔
2	ذخیرہ کرنے کی جگہ میں ڈیٹا چھپا ہوا ہے۔	مجرم عام طور پر سسٹم کمانڈز اور پروگرامز کا استعمال کرتے ہوئے پوشیدہ شکل میں سٹوریج میڈیم کے اندر ڈیٹا کے ٹکڑوں کو چھپاتے ہیں۔
3	خفیہ چینل	ایک خفیہ چینل ایک مواصلاتی پروٹوکول ہے جو حملہ آور کو مداخلت کا پتہ لگانے کی تکنیک کو نظرانداز کرنے اور نیٹ ورک پر ڈیٹا چھپانے کی اجازت دیتا ہے۔ حملہ آور نے اسے آپس میں تعلق چھپانے کے لیے استعمال کیا۔ وہ اور سمجھوتہ شدہ نظام۔

دیگر تکنیکی چیلنجز ہیں:

بادل میں کام کرنا

ڈیٹا کو محفوظ کرنے کا وقت

مہارت کا فرق

سٹیگنو گرافی

قانونی چیلنجز

ڈیجیٹل شواہد کی پیش کش اس کے جمع کرنے سے زیادہ مشکل ہے کیونکہ ایسی بہت سی مثالیں ہیں جہاں قانونی فریم ورک نرم رویہ اختیار کرتا ہے اور سائبر فرانزک کے ہر پہلو کو تسلیم نہیں کرتا، جیسا کہ جگدیو سنگھ V. ریاست اور Ors دہلی ہائی کورٹ نے اس کا فیصلہ کیا۔

"سی ڈی اور سی ڈی آر میں ایک مداخلت شدہ ٹیلی فون کال کے قابل قبولیت سے نمٹنے کے دوران جو سیکشن کے تحت سرٹیفکیٹ کے بغیر تھا۔ انڈین ایویڈنس ایکٹ 1872 کے 65B کے تحت عدالت نے مشاہدہ کیا کہ ثانوی الیکٹرانک ثبوت بغیر سرٹیفکیٹ کے۔ انڈین ایویڈینس ایکٹ، 1872 کی 65B قابل قبول نہیں ہے اور کسی بھی مقصد کے لیے عدالت اسے نہیں دیکھ سکتی۔ یہ زیادہ تر معاملات میں ہوتا ہے کیونکہ سائبر پولیس کے پاس ثبوت کے ممکنہ ذریعہ کی نشاندہی کرنے اور اسے ثابت کرنے کی ضروری اہلیت اور صلاحیت کا فقدان ہے۔ اس کے علاوہ، زیادہ تر وقت الیکٹرانک شواہد کو اس کی دیانتداری کی وجہ سے عدالت میں چیلنج کیا جاتا ہے۔ مناسب رہنما خطوط کی عدم موجودگی اور مجموعے کی صحیح وضاحت کی عدم موجودگی، اور الیکٹرانک شواہد کا حصول خود ہی خارج ہو جاتا ہے۔

قانونی چیلنجز

S.No.	قسم	تفصیل
	رہنما اصولوں اور معیارات کی عدم موجودگی	ہندوستان میں، ڈیجیٹل ثبوت جمع کرنے اور حاصل کرنے کے لیے کوئی مناسب رہنما اصول نہیں ہیں۔ تحقیقاتی ایجنسیاں اور فرانزک لیبارٹریز اپنے گائیڈ لائن پر کام کر رہی ہیں۔ اس کی وجہ سے، ڈیجیٹل ثبوت کی صلاحیت کو تباہ کر دیا گیا ہے.
	حد بندی کی دی انڈین ایویڈینس ایکٹ، 1872	انڈین ایویڈنس ایکٹ، 1872 کا نقطہ نظر محدود ہے، یہ وقت کے ساتھ تیار نہیں ہو پا رہا ہے اور ای شواہد سے چھیڑ چھاڑ، تبدیلی، ٹرانسپوزیشن وغیرہ کا زیادہ خطرہ ہے۔ قانون ای شواہد جمع کرنے کے طریقہ کار پر خاموش ہے۔ یہ صرف سیکشن کے ذیلی دفعہ 4 کے مطابق ایک سرٹیفکیٹ کے ساتھ عدالت میں الیکٹرانک ثبوت پیش کرنے پر توجہ مرکوز کرتا ہے۔ 65B[12].اس کا مطلب یہ ہے کہ اس سے کوئی فرق نہیں پڑتا ہے کہ کسی بھی طریقہ کار پر عمل کیا جاتا ہے اسے a کی مدد سے ثابت کیا جانا چاہئے۔ سرٹیفکیٹ

دیگر قانونی چیلنجز

رازداری کے مسائل

عدالتوں میں قابل قبولیت

الیکٹرانک ثبوت کا تحفظ

ڈیجیٹل ثبوت جمع کرنے کی طاقت

چلتے ہوئے کمپیوٹر کا تجزیہ کرنا

وسائل کے چیلنجز

جیسے جیسے جرائم کی شرح میں اضافہ ہوتا ہے ڈیٹا کی تعداد میں اضافہ ہوتا ہے اور اتنے بڑے ڈیٹا کا تجزیہ کرنے کا بوجھ بھی ڈیجیٹل فرانزک ماہر پر بڑھتا ہے کیونکہ ڈیجیٹل ثبوت جسمانی شواہد کے مقابلے میں زیادہ حساس ہوتے ہیں یہ آسانی سے غائب ہو سکتے ہیں۔ تفتیشی عمل کو تیز اور کارآمد بنانے کے لیے فرانزک ماہرین ڈیٹا کی صداقت کو جانچنے کے لیے مختلف ٹولز استعمال کرتے ہیں لیکن ان ٹولز سے نمٹنا بھی اپنے آپ میں ایک چیلنج ہے۔

4.9 وسائل کے چیلنجز کی اقسام

ٹیکنالوجی میں تبدیلی

آپریٹنگ سسٹمز، ایپلیکیشن سافٹ ویئر اور ہارڈ ویئر جیسی ٹیکنالوجی میں تیزی سے تبدیلی کی وجہ سے ڈیجیٹل شواہد کو پڑھنا زیادہ مشکل ہوتا جا رہا ہے کیونکہ نئے ورژن کے سافٹ ویئر زپرانے ورژن کے لیے سپورٹ نہیں ہوتے اور سافٹ ویئر تیار کرنے والی کمپنیوں نے کوئی بیکورڈ کمپیٹیبل فراہم نہیں کیا جو قانونی طور پر بھی متاثر ہوتا ہے۔

حجم اور نقل

الیکٹرانک دستاویزات کی رازداری، دستیابی، اور سالمیت کو آسانی سے جوڑ دیا جاتا ہے۔ وسیع ایریا نیٹ ورکس اور انٹرنیٹ کا امتزاج ایک بڑا نیٹ ورک بناتا ہے جو ڈیٹا کو جسمانی حدود سے باہر بہانے کی اجازت دیتا ہے۔ مواصلات کی اتنی آسانی اور الیکٹرانک دستاویز کی دستیابی سے ڈیٹا کا حجم بڑھ جاتا ہے جس سے اصل اور متعلقہ ڈیٹا کی شناخت میں بھی دشواری پیدا ہوتی ہے۔

4.10 اکتسابی نتائج

- سائبر اسپیس کی تعریف اور اس کی خصوصیات بیان کر سکے گا۔
- سائبر اسپیس میں بین الاقوامی قوانین کی اہمیت سمجھ سکے گا۔
- سائبر کرائم سے متعلق بین الاقوامی قانونی فریم ورک کی وضاحت کر سکے گا۔
- سائبر فارنزکس کی ضرورت اور اہمیت بیان کر سکے گا۔
- ای میل کے فارنزک تجزیے میں استعمال ہونے والی معلومات کو سمجھ سکے گا۔
- مختلف Email Forensic Tools کی وضاحت کر سکے گا۔

- Digital Forensics Lifecycle کے مراحل Collection، Examination، Analysis اور Reporting بیان کر سکے گا۔

4.11 کلیدی الفاظ

- سائبر اسپیس — Cyberspace
- بین الاقوامی قانون — International Law
- سائبر کرائم — Cybercrime
- سائبر فارنزکس — Cyber Forensics
- ڈیجیٹل فارنزکس — Digital Forensics
- ای میل فارنزکس — Email Forensics
- فارنزک تحقیقات — Forensic Investigation
- نیٹ ورک ڈیوائس تفتیش — Network Device Investigation
- Email Header
- IP Address
- X-Mailer
- MiTec Mail Viewer

4.12 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1۔ سائبر اسپیس سے کیا مراد ہے؟

2۔ سائبر فارنزکس کیا ہے؟

3۔ ای میل فارنزکس کیا ہے؟

4۔ Anti-Forensics کیا ہے؟

5۔ Digital Forensics Lifecycle کیا ہے؟

مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1۔ سائبر اسپیس کی تعریف کریں اور اس کی اہمیت بیان کریں۔

2۔ سائبر کرائم کے لیے بین الاقوامی قانون کے کردار کی وضاحت کریں۔

3۔ سائبر فارنزکس کیا ہے؟ اس کی اہمیت بیان کریں۔

4۔ ای میل کے فارنزک تجزیے کے مختلف طریقوں کی وضاحت کریں۔

5۔ کسی بھی تین Email Forensic Tools کی وضاحت کریں۔

6۔ Digital Forensics Lifecycle کے مختلف مراحل کی وضاحت کریں۔

7۔ فارنزک تحقیقات کی مختلف اقسام بیان کریں۔

8۔ ڈیجیٹل فارنزکس کو درپیش تکنیکی، قانونی اور وسائل کے چیلنجز کی وضاحت کریں۔

طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1۔ سائبر فارنزکس کی تعریف اور اہمیت بیان کریں۔ ای میل فارنزک تجزیہ، مختلف فارنزک ٹولز اور Digital Forensics Lifecycle کی تفصیل سے وضاحت کریں۔

2۔ Digital Forensics کیا ہے؟ Forensic Investigation کے مختلف مراحل کی وضاحت کرتے ہوئے Collection، Examination، Analysis اور Reporting کو تفصیل سے بیان کریں۔

3۔ ڈیجیٹل فارنزکس کو درپیش مختلف چیلنجز کی تفصیل سے وضاحت کریں۔ تکنیکی چیلنجز، قانونی چیلنجز اور وسائل کے چیلنجز کے ساتھ Anti-Forensics Techniques کو بھی بیان کریں۔

4.13 تجویز کردہ اکتسابی مواد

1۔ سائبر اسپیس میں بین الاقوامی قوانین کا کردار

2۔ سائبر کرائم کے لیے بین الاقوامی قانون

3۔ سائبر فارنزکس کا تعارف

4۔ ای میل کا فارنزک تجزیہ

5۔ Email Forensic Tools

6۔ Digital Forensics Lifecycle

7۔ Forensic Investigation

8۔ Computer/Cyber Forensics

9۔ Digital Forensics کے تکنیکی چیلنجز

10۔ Digital Forensics کے قانونی چیلنجز

11۔ Digital Forensics کے وسائل سے متعلق چیلنجز

12۔ Anti-Forensics Techniques

اکائی 5۔ سائبر کرائمز: موبائل اور وائرلیس ڈیوایسز

اکائی کے اجزاء

5.0 تمہید

5.1 مقاصد

5.2 تعارف

5.3 موبائل اور وائرلیس کمپیوٹنگ کے دور میں کریڈٹ کارڈ فراڈ:

5.4 موبائل آلات کے ذریعہ درپیش سیکیورٹی چیلنجز:

5.5 موبائل آلات کے لیے رجسٹری کی ترتیبات:

5.6 موبائل- سیل فونز پر (Attacks):

5.7 موبائل کمپیوٹنگ کے دور میں تنظیمی سیکورٹی کی پالیسیاں اور اقدامات:

5.8 اکتسابی نتائج

5.9 کلیدی الفاظ

5.10 نمونہ امتحانی سوالات

5.11 تجویز کردہ اکتسابی مواد

5.0 تمہید

موبائل اور وائرلیس کمپیوٹنگ نے ہماری روزمرہ اور کاروباری زندگی کو بہت آسان بنادیا ہے۔ موبائل آلات کے ذریعے ای میل، بینکنگ، شاپنگ اور کارپوریٹ نیٹ ورکس تک رسائی ممکن ہے۔ تاہم، ان آلات کے بڑھتے ہوئے استعمال کے ساتھ سیکیورٹی کے خطرات بھی بڑھ رہے ہیں۔ موبائل آلات گم یا چوری ہو سکتے ہیں اور ان میں موجود ذاتی اور کاروباری معلومات غیر مجاز افراد تک پہنچ سکتی ہیں۔

5.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- موبائل اور وائرلیس کمپیوٹنگ کے بنیادی تصور کو سمجھ سکے گا۔

- موبائل کمپیوٹنگ میں کریڈٹ کارڈ فراڈ کی وضاحت کر سکے گا۔
- موبائل آلات کو درپیش مختلف سیکیورٹی چیلنجز کو بیان کر سکے گا۔
- موبائل آلات کی رجسٹری سیٹنگز اور Authentication Service Security کو سمجھ سکے گا۔
- موبائل فونز پر ہونے والے مختلف حملوں کی وضاحت کر سکے گا۔
- موبائل وائرس، Malware، DoS، Overbilling اور دیگر حملوں کو سمجھ سکے گا۔
- تنظیمی موبائل سیکیورٹی پالیسیوں کی اہمیت بیان کر سکے گا۔

5.2 تعارف

کیوں چاہئے موبائل آلات محفوظ کیا جائے؟ ہر روز، موبائل آلات کھوئے ہوئے، چوری ہوئے، اور متاثر ہوئے۔ موبائل آلات اہم کاروباری اور ذاتی ذخیرہ کر سکتے ہیں معلومات، اور اکثر یونیورسٹی سسٹمز، ای میل، بینکنگ تک رسائی کے لیے استعمال ہوتے ہیں۔

موبائل اور وائرلیس آلات کا پھیلاؤ:

لوگ کیفے، ہوائی اڈوں، سپر مارکیٹوں اور یہاں تک کہ بس اسٹاپوں پر بھی اپنے اسمارٹ فونز یا ٹیبلیٹس پر گھومتے ہیں، بظاہر کسی بھی چیز یا اپنے آس پاس کے کسی سے غافل نظر آتے ہیں۔

وہ گیم کھیلتے ہیں، ای میل ڈاؤن لوڈ کرتے ہیں، شاپنگ پر جاتے ہیں یا چلتے پھرتے اپنے بینک بیلنس چیک کرتے ہیں۔

وہ کارپوریٹ نیٹ ورکس تک بھی رسائی حاصل کر سکتے ہیں اور اپنے موبائل گیجٹس پر ایک یادو دستاویز کھینچ سکتے ہیں۔

آج، موبائل آلات کے لئے ناقابل یقین ترقی کی جارہی ہے. یہ رجحان چھوٹے آلات اور زیادہ پروسیسنگ پاور کے لیے ہے۔ کچھ سال پہلے، انتخاب ایک وائرلیس فون اور ایک سادہ PDA کے درمیان تھا۔ اب خریداروں کے پاس انٹیگریٹڈ وائرلیس موڈیم کے ساتھ اعلیٰ درجے کے PDAs اور وائرلیس ویب براؤزنگ کی صلاحیتوں والے چھوٹے فونز کے درمیان انتخاب ہے۔ موبائل صارفین کے لیے اختیارات کی ایک طویل فہرست دستیاب ہے۔ ایک سادہ ہاتھ سے پکڑا ہوا موبائل ڈیوائس چھوٹی ایپلی کیشنز چلانے، گیمز اور میوزک چلانے اور وائس کال کرنے کے لیے کافی کمپیوٹنگ پاور فراہم کرتا ہے۔ موبائل ٹکنالوجی کی ترقی کا ایک اہم محرک کاروباری حلوں کا ہاتھ سے پکڑے گئے آلات میں تیزی سے اضافہ ہے۔

جیسا کہ اصطلاح "موبائل ڈیوائس" میں بہت سی مصنوعات شامل ہیں۔ ہم سب سے پہلے کلیدی اصطلاحات میں واضح فرق فراہم کرتے ہیں: موبائل کمپیوٹنگ، وائرلیس کمپیوٹنگ اور ہینڈ ہیلڈ ڈیوائسز۔ نیچے دی گئی تصویر ہمیں یہ سمجھنے میں مدد کرتی ہے کہ یہ شرائط کیسے متعلق ہیں۔ آیئے موبائل کمپیوٹنگ کے تصور اور مختلف قسم کے آلات کو سمجھتے ہیں۔

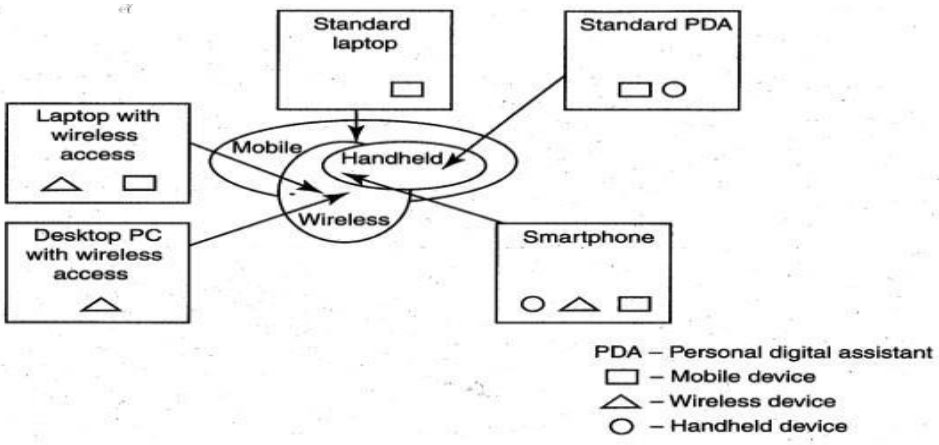


Figure : Mobile, Wireless and hand-held Devices

موبائل کمپیوٹنگ "کمپیوٹر اور تمام ضروری فائلوں اور سافٹ ویئر کو فیلڈ میں لے جانا ہے۔" 1990 کی دہائی سے کئی قسم کے موبائل کمپیوٹر متعارف کرائے گئے ہیں۔ وہ درج ذیل ہیں:

- پورٹ ایبل کمپیوٹر: یہ ایک عام مقصد والا کمپیوٹر ہے جسے آسانی سے ایک جگہ سے دوسری جگہ منتقل کیا جا سکتا ہے، لیکن ٹرانزٹ کے دوران استعمال نہیں کیا جا سکتا، عام طور پر اس لیے کہ اسے کچھ "سیٹ اپ" اور AC پاور سورس کی ضرورت ہوتی ہے۔
- ٹیبلٹ پی سی: اس میں کی بورڈ کی کمی ہے، جس کی شکل سلیٹ یا کاغذی نوٹ بک کی طرح ہے اور اس میں اسٹائلس اور ہینڈ رائٹنگ ریکگنیشن سافٹ ویئر کے ساتھ ٹچ اسکرین کی خصوصیات ہیں۔ ٹیبلیٹس ان ایپلی کیشنز کے لیے بہترین موزوں نہیں ہو سکتے جن کو ٹائپنگ کے لیے فزیکل کی بورڈ کی ضرورت ہوتی ہے، لیکن دوسری صورت میں یہ زیادہ تر کاموں کو انجام دینے کے قابل ہیں جو ایک عام لیپ ٹاپ انجام دے سکتا ہے۔
- انٹرنیٹ ٹیبلٹ: یہ ٹیبلٹ کی شکل میں انٹرنیٹ کا آلہ ہے۔ ٹیبلٹ پی سی کے برعکس، انٹرنیٹ ٹیبلیٹ میں کمپیوٹنگ کی زیادہ طاقت نہیں ہے اور اس کا ایپلی کیشن سوٹ محدود ہے۔ یہ بھی نہیں ہو سکتا عام مقصد کے کمپیوٹر کو تبدیل کریں۔ انٹرنیٹ ٹیبلٹس میں عام طور پر ایک MP3 اور ویڈیو پلیئر، ایک ویب براؤزر، ایک چیٹ ایپلی کیشن اور تصویر دیکھنے والا ہوتا ہے۔
- پرسنل ڈیجیٹل اسسٹنٹ (PDA): یہ ایک چھوٹا، عام طور پر جیب کے سائز کا، محدود فعالیت والا کمپیوٹر ہے۔ اس کا مقصد ایک ڈیسک ٹاپ کمپیوٹر کے ساتھ ہم آہنگی پیدا کرنا اور رابطوں، ایڈریس بک، نوٹس، ای میل اور دیگر خصوصیات تک رسائی دینا ہے۔
- الٹرا موبائل (پی سی): یہ ایک مکمل خصوصیات والا، PDA کے سائز کا کمپیوٹر ہے جو عام مقصد کے آپریٹنگ سسٹم (OS) کو چلاتا ہے۔
- اسمارٹ فون: یہ ایک مربوط سیل فون فعالیت کے ساتھ ایک PDA ہے۔ موجودہ سمارٹ فونز میں بہت ساری خصوصیات اور انسٹالیبل ایپلی کیشنز ہیں۔
- کار پیوٹر: یہ ایک آٹو موبائل میں نصب ایک کمپیوٹنگ ڈیوائس ہے۔ یہ وائرلیس کمپیوٹر، ساؤنڈ سسٹم، گلوبل پوزیشننگ سسٹم (GPS) اور DVD پلیئر کے طور پر کام کرتا ہے۔ اس میں ورڈ پروسیسنگ سافٹ ویئر بھی شامل ہے اور یہ بلوٹوتھ سے مطابقت رکھتا ہے۔

- فلائی فیوژن پینٹ ٹاپ کمپیوٹر: یہ ایک کمپیوٹنگ ڈیوائس ہے جس کا سائز اور شکل قلم ہے۔ یہ تحریری برتن، MP3 پلیئر، لینگویج ٹرانسلیٹر، ڈیجیٹل اسٹوریج ڈیوائس اور کیلکولیٹر کے طور پر کام کرتا ہے۔

نقل و حرکت کے رجحانات:

موبائل کمپیوٹنگ ایک نئے دور، تھرڈ جنریشن (3G) میں منتقل ہو رہی ہے، جو ایپلی کیشنز میں وسیع اقسام کا وعدہ کرتی ہے اور اس کے استعمال کے ساتھ ساتھ تیز رفتار نیٹ ورکنگ میں بھی بہتری آئی ہے۔ ایپل کے "iPhone" اور Google کی قیادت میں "Android" فونز اس رجحان کی بہترین مثالیں ہیں اور اس سمت میں بہت ساری دیگر پیشرفتیں ہیں۔ یہ سمارٹ موبائل ٹیکنالوجی تیزی سے مقبولیت حاصل کر رہی ہے اور حملہ آور (ہیکرز اور کریکرز) اس کے سب سے بڑے مداحوں میں شامل ہیں۔

یہ موبائل کمپیوٹنگ میں رجحانات کو نوٹ کرنے کے قابل ہے؛ اس سے قارئین سے قارئین کو موبائل کمپیوٹنگ ڈومین میں سائبر سیکیورٹی (Cyber security) کے مسائل کی سنگینی کا احساس کرنے میں مدد ملے گی۔ نیچے دی گئی تصویر نقل و حرکت کی مختلف اقسام اور ان کے اثرات کو ظاہر کرتی ہے۔

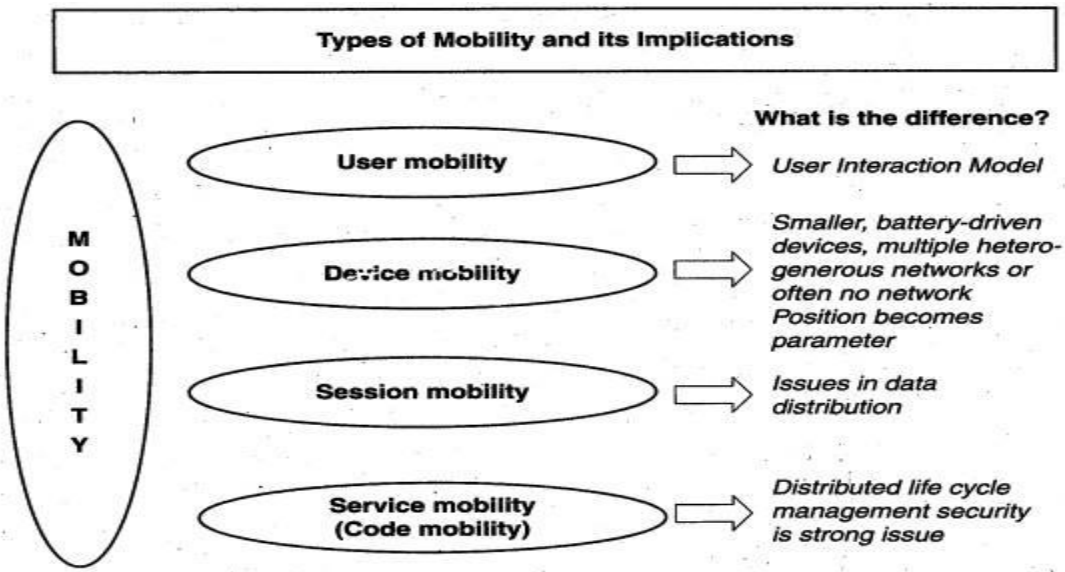


Figure: Mobility types and implications

نئی ٹیکنالوجی 3G نیٹ ورک مکمل طور پر آئی پی ڈیٹا سیکیورٹی کے ساتھ نہیں بنائے گئے ہیں۔ مزید برآں، آئی پی ڈیٹا کی دنیا جب آواز پر مبنی سیکیورٹی خطرات کے مقابلے میں موبائل آپریٹرز کے لیے نئی ہے۔ ہیں متعدد (Attacks) جو موبائل نیٹ ورکس کے خلاف کیے جا سکتے ہیں اور وہ دو بنیادی ویکٹرز سے شروع ہو سکتے ہیں۔ ایک موبائل نیٹ ورک کے باہر سے ہے - یعنی پبلک انٹرنیٹ، پرائیویٹ نیٹ ورکس اور دوسرے آپریٹر کے نیٹ ورکس - اور دوسرا موبائل نیٹ ورکس کے اندر ہے - یعنی ڈیٹا کے قابل ہینڈ سیٹس اور سمارٹ فونز، نوٹ بک کمپیوٹرز یا یہاں تک کہ ڈیسک ٹاپ کمپیوٹرز بھی جڑے ہوئے ہیں۔ 3G نیٹ ورک پر۔

3G موبائل نیٹ ورکس کے خلاف حملوں کی مقبول اقسام درج ذیل ہیں:

مالویئر، وائرس اور کیڑے: اگرچہ بہت سے صارفین اب بھی 2G, 2.5G 2G, 2.5G سے 3G, 3G میں تبدیل ہونے کے

عارضی عمل میں ہیں، لیکن کمیونٹی(community) کے لوگوں کو تعلیم دینے اور موبائل آلات کے استعمال کے دوران موجود ایسے خطرات کے بارے میں آگاہی فراہم کرنے کی ایک بڑھتی ہوئی ضرورت ہے۔ موبائل آلات کے لیے مخصوص میلویئر کی چند مثالیں یہ ہیں:

- Skull Trojan: میں Symbian موبائل OS سے لیس سیریز 60 فونز کو نشانہ بناتا ہوں۔
- Cabir Trojan: یہ پہلا وقف شدہ موبائل فون ورم ہے جو Symbian OS پر چلنے والے فونز کو متاثر کرتا ہے اور دوسرے موبائل آلات کو اسکین کرتا ہے تاکہ اس کی ایک کاپی بلوٹوتھ وائرلیس ٹیکنالوجی کے ذریعے ملنے والے پہلے کمزور فون کو بھیج سکے۔ اس کیڑے کی سب سے بری بات یہ ہے کہ Cabir-H اور Cabir-I وائرس کا سورس کوڈ آن لائن دستیاب ہے۔
- mosquito Trojan: یہ سیریز 60 اسمارٹ فونز کو متاثر کرتا ہے اور یہ "Mosquitos" موبائل فون گیم کا کریک ورژن ہے۔
- Brador torjan: یہ svchost بنا کر Windows CE OS کو متاثر کرتا ہے۔ ونڈوز اسٹارٹ اپ فولڈر میں exe فائل جو ڈیوائس کے مکمل کنٹرول کی اجازت دیتی ہے۔ یہ قابل عمل فائل روایتی کیڑے کے پھیلاؤ کے ویکٹر جیسے ای میل فائل اٹیچمنٹ کے لیے قابل عمل ہے۔
- Lasco worm: یہ سب سے پہلے 2005 میں PDAs اور Symbian OS چلانے والے موبائل فونز کو نشانہ بنانے کے لیے جاری کیا گیا تھا۔ Lasco Cabir کے سورس کوڈ پر مبنی ہے اور بلوٹوتھ کنکشن پر نقل کرتا ہے۔
- سروس سے انکار (Denial-of-service DoS): اس (Attacks) کے پیچھے بنیادی مقصد یہ ہے کہ سسٹم کو مطلوبہ صارفین کے لیے دستیاب نہ کیا جائے۔ سسٹم کو غیر دستیاب بنانے کے لیے وائرس کے (Attacks) سسٹم کو نقصان پہنچانے کے لیے استعمال کیے جا سکتے ہیں۔ اس وقت، وائرڈ انٹرنیٹ سروس پرووائیڈرز (iSPs) کے لیے سب سے زیادہ عام سائبر سیکیورٹی (Cyber security) خطرات میں سے ایک ڈسٹری بیوٹڈ ڈینیئل آف سروس (DDos) حملہ ہے۔ DDoS حملوں کا استعمال ٹارگٹ سسٹم کو ڈیٹا سے بھرنے کے لیے کیا جاتا ہے تاکہ ہدف کی جانب سے جوابی کارروائی کی جا سکے۔ نظام یا تو سست یا بند ہے.
- Overbilling attack: اوور بلنگ میں حملہ آور ایک سبسکرائبر کا IP ایڈریس ہائی جیک کرتا ہے اور پھر اسے (یعنی کنکشن) کا استعمال کرتے ہوئے ایسے ڈاؤن لوڈز شروع کرتا ہے جو "مفت ڈاؤن لوڈز" نہیں ہیں یا اسے اپنے مقاصد کے لیے استعمال کرتے ہیں۔ دونوں صورتوں میں، جائز صارف سے اس سرگرمی کا معاوضہ لیا جاتا ہے جسے صارف نے انجام نہیں دیا یا کرنے کا اختیار نہیں دیا۔
- جعلی پالیسی کی ترقی کا عمل (Spoofed policy development process PDP): یہ GTP (Attacks) [جنرل پیکٹ ریڈیو سروس (GPRS) ٹنلنگ پروٹوکول] میں موجود کمزوریوں کا فائدہ اٹھاتے ہیں۔
- Signaling-level attacks: سیشن انیشیشن پروٹوکول (SIP) ایک سگنلنگ پروٹوکول ہے جو IP ملٹی میڈیا سب سسٹم (IMS) نیٹ ورکس میں وائس اوور انٹرنیٹ پروٹوکول (VoIP) خدمات فراہم کرنے کے لیے استعمال ہوتا ہے۔ SIP پر مبنی VolP سسٹمز میں کئی کمزوریاں ہیں۔

5.3 موبائل اور وائرلیس کمپیوٹنگ کے دور میں کریڈٹ کارڈ فراڈ

یہ سائبر کرائم کے نئے رجحانات ہیں جو موبائل کمپیوٹنگ کے ساتھ آرہے ہیں - موبائل کامرس (M-Commerce) اور موبائل بینکنگ (M-Banking)۔ موبائل ہینڈ ہیلڈ ڈیوائسز کی مسلسل بڑھتی ہوئی طاقت اور مسلسل کم ہوتی قیمتوں کے پیش نظر کریڈٹ کارڈ کے فراڈ اب عام ہوتے جارہے ہیں، جن کے نتیجے میں تقریباً کسی کو بھی ان گیجٹس کی آسانی سے دستیابی ہوتی ہے۔ آج کا تعلق "موبائل کمپیوٹنگ" سے ہے، یعنی کہیں بھی کسی بھی وقت کمپیوٹنگ۔ وائرلیس ٹکنالوجی میں ہونے والی پیشرفت نے سفید کالر کارکنوں کے کام کرنے کے اس نئے انداز کو ہوا دی ہے۔ یہ کریڈٹ کارڈ پروسیسنگ کے لیے بھی درست ہے۔ وائرلیس کریڈٹ کارڈ پروسیسنگ ہے

نسبتاً نئی سروس جو کسی شخص کو کریڈٹ کارڈز کو الیکٹرانک طور پر، عملی طور پر کہیں بھی پروسیس کرنے کی اجازت دے گی۔ وائرلیس کریڈٹ کارڈ پروسیسنگ ایک انتہائی مطلوبہ نظام ہے، کیونکہ یہ کاروباروں کو موبائل مقامات سے لین دین کو تیزی سے، موثر اور پیشہ ورانہ طریقے سے پروسیس کرنے کی اجازت دیتا ہے۔ یہ اکثر ایسے کاروباروں کے ذریعہ استعمال ہوتا ہے جو بنیادی طور پر موبائل ماحول میں کام کرتے ہیں۔

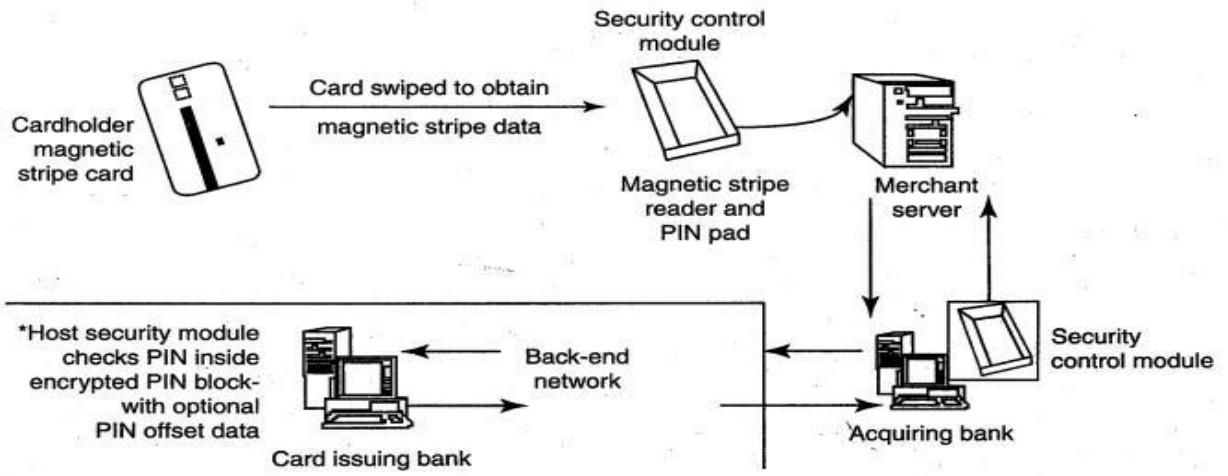


Figure : Online environment for credit card transactions

ایک آسٹریلوی کمپنی "Alacrity" سے ایک سسٹم دستیاب ہے جسے کلوزڈ لوپ انوائرمنٹ فار وائرلیس (CLEW) کہتے ہیں۔ اوپر کی تصویر CLEW کے ساتھ واقعات کے بہاؤ کو ظاہر کرتی ہے جو Alacrity کا رجسٹرڈ ٹریڈ مارک ہے جو یہاں صرف اس ماحول میں بہاؤ کو ظاہر کرنے کے لیے استعمال کیا جاتا ہے۔

جیسا کہ شکل میں دکھایا گیا ہے، بنیادی بہاؤ مندرجہ ذیل ہے:

- مرچنٹ بینک کو لین دین بھیجتا ہے۔
- بینک درخواست کو مجاز کارڈ ہولڈر تک پہنچاتا ہے۔
- کارڈ ہولڈر منظور یا مسترد کرتا ہے (پاس ورڈ سے محفوظ)

- بینک/مرچنٹ کو مطلع کیا جاتا ہے۔
- کریڈٹ کارڈ کا لین دین مکمل ہو گیا ہے۔

5.4 موبائل آلات کے ذریعہ درپیش سیکیورٹی چیلنجز

موبلٹی سائبر سیکیوریٹی کے لیے دو اہم چیلنجز لاتی ہے: پہلا، ہاتھ سے پکڑے گئے آلات پر، معلومات کو جسمانی طور پر کنٹرول شدہ ماحول سے باہر لے جایا جارہا ہے اور دوسرا محفوظ ماحول تک ریموٹ رسائی کی اجازت دی جارہی ہے۔ سائبر سیکیوریٹی کے ان چیلنجوں کے بارے میں تنظیموں کے تاثرات مناسب سیکورٹی آپریٹنگ طریقہ کار وضع کرنے میں اہم ہیں۔ جب لوگوں سے موبائل آلات کی متنوع رینج کے انتظام میں اہم کے بارے میں پوچھا جاتا ہے، تو ایسا لگتا ہے کہ وہ ذیل کے اعداد و شمار میں دکھائے گئے آلات کے بارے میں سوچ رہے ہیں۔

جیسے جیسے موبائل ڈیوائس استعمال کرنے والوں کی تعداد میں اضافہ ہوتا ہے، دو چیلنجز پیش کیے جاتے ہیں: ایک ڈیوائس کی سطح پر جسے "مائیکرو چیلنجز" کہا جاتا ہے اور دوسرا تنظیمی سطح پر جسے "میکرو چیلنجز" کہا جاتا ہے۔

موبائل سیکیورٹی میں کچھ معروف تکنیکی چیلنجز یہ ہیں: رجسٹری کی ترتیبات اور کنفیگریشنز کا انتظام، تصدیقی سروس سیکیورٹی، کرپٹو گرافی سیکیورٹی، لائٹ ویٹ ڈائرکٹری ایکسیس پروٹوکول (LDAP) سیکیورٹی، ریموٹ ایکسیس سرور (RAS) سیکیورٹی، میڈیا پلیئر کنٹرول سیکیورٹی، نیٹ ورکنگ ایپلیکیشن پروگرام۔انٹرفیس (API)، سیکورٹی وغیرہ

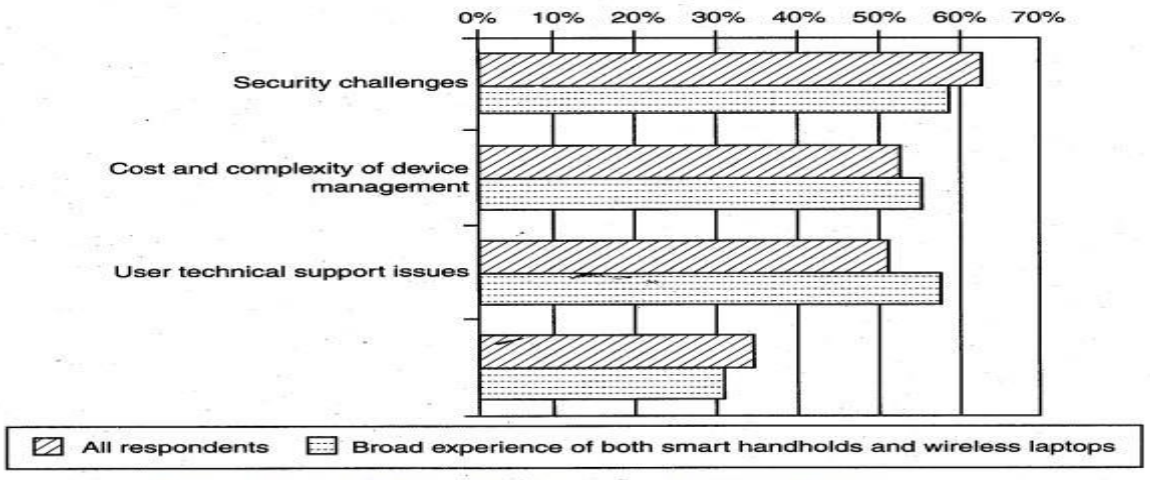


Figure: Important issues for managing mobile devices

5.5 موبائل آلات کے لیے رجسٹری کی ترتیبات

آیئے موبائل ڈیوائسز پر رجسٹری سیٹنگز کے مسئلے کو ایک مثال کے ذریعے سمجھتے ہیں: Microsoft Activesync کا

مقصد ونڈوز سے چلنے والے پرسنل کمپیوٹرز (PCs) اور Microsoft Outlook کے ساتھ مطابقت پذیری کے لیے ہے۔ "Windows ActiveSync سے چلنے والے PC اور Windows موبائل سے چلنے والے ڈیوائس کے درمیان گیٹ وے کے طور پر کام کرتا ہے، جس سے ایپلیکیشنز جیسے Outlook کی معلومات، Microsoft Office دستاویزات، تصاویر، موسیقی، ویڈیوز اور ایپلیکیشنز کو صارف کے ڈیسک ٹاپ سے اس کے ڈیوائس پر منتقل کیا جاسکتا ہے۔

پی سی کے ساتھ ہم وقت سازی کے علاوہ، ActiveSync براہ راست مائیکروسافٹ ایکسچینج سرور کے ساتھ ہم وقت سازی کر سکتا ہے تاکہ صارف اپنے ای میلز، کیلنڈر، نوٹس اور رابطوں کو وائرلیس طریقے سے اپ ڈیٹ کر سکیں جب وہ اپنے پی سی سے دور ہوں۔ اس تناظر میں، رجسٹری کی ترتیب اس آسانی کے پیش نظر ایک اہم مسئلہ بن جاتی ہے جس کے ساتھ مختلف ایپلی کیشنز معلومات کے آزادانہ بہاؤ کی اجازت دیتی ہیں۔

توثیق سروس سیکورٹی (Authentication Service security):

موبائل کمپیوٹنگ میں سیکیورٹی کے دو اجزاء ہیں: ڈیوائسز کی سیکیورٹی اور نیٹ ورکس میں سیکیورٹی۔ ایک محفوظ نیٹ ورک تک رسائی میں ڈیوائس اور بیس اسٹیشنز یا ویب سرور (web server) کے درمیان تصدیق شامل ہوتی ہے۔ یہ اس بات کو یقینی بنانے کے لیے ہے کہ درخواست کردہ خدمات حاصل کرنے کے لیے صرف تصدیق شدہ آلات ہی نیٹ ورک سے منسلک ہوں۔ کوئی بھی بدنیتی پر مبنی کوڈ سروس فراہم کنندہ کی نقالی نہیں کر سکتا تاکہ آلہ کو ایسا کچھ کرنے کے لیے دھوکہ دے جس کا اس کا مطلب نہ ہو۔ اس طرح، نیٹ ورک موبائل آلات کی حفاظت میں بھی اہم کردار ادا کرتے ہیں۔

کچھ نمایاں قسم کے (Attacks) جن کا موبائل ڈیوائسز کو نشانہ بنایا جاتا ہے وہ ہیں: پش اٹیک، پل اٹیک اور کریش اٹیک۔

وائرلیس نیٹ ورکس کے ذریعے موبائل آلات پر عام حملوں کے پیش نظر تصدیقی خدمات کی حفاظت اہم ہے: ڈاس (Attacks)، ٹریفک کا تجزیہ، چھپنا، درمیان میں آدمی کے (Attacks) اور سیشن ہائی جیکنگ۔ اس منظر نامے میں حفاظتی اقدامات وائرلیس ایپلیکیشن پروٹوکول VPNs، (WAPs) کے استعمال، میڈیا ایکسیس کنٹرول (MAC) ایڈریس فلٹرنگ اور xx.802 معیارات میں ترقی سے آتے ہیں۔

5.6 موبائل - سیل فونز پر (Attacks)

موبائل فون چوری:

موبائل فون ہر کسی کی زندگی کا ایک لازمی حصہ بن گیا ہے اور موبائل فون ایک عیش و آرام سے ایک ننگی ضرورت میں بدل گیا ہے۔ قوت خرید میں اضافہ اور متعدد کم قیمت ہینڈ سیٹس کی دستیابی بھی موبائل فون استعمال کرنے والوں میں اضافے کا باعث بنی ہے۔ گزشتہ چند سالوں میں موبائل فونز کی چوری میں ڈرامائی طور پر اضافہ ہوا ہے۔ چونکہ بہت بڑا ہندوستان میں کام کرنے والی آبادی کا ایک حصہ پبلک ٹرانسپورٹ کا استعمال کرتا ہے، جن اہم مقامات پر چوری ہوتی ہے وہ بس اسٹاپ، ریلوے اسٹیشن اور ٹریفک سگنلز ہیں۔

مندرجہ ذیل عوامل موبائل آلات پر پھیلنے میں معاون ہیں:

کافی ہدف والے ٹرمینلز: پام اوایس ڈیوائسز کی تعداد 15 ملین تک پہنچنے کے بعد پہلا پام اوایس وائرس دیکھا گیا۔ موبائل وائرس کی پہلی مثال جون 2004 کے دوران دیکھی گئی جب یہ پتہ چلا کہ ایک تنظیم "Ojam" نے اپنے موبائل فون گیم کے پرانے ورژن میں ایک اینٹی پائریسی ٹروجن وائرس تیار کیا ہے جسے Mosquito کہا جاتا ہے۔ اس وائرس نے صارفین کے علم میں لائے بغیر تنظیم کو ایس ایم ایس ٹیکسٹ پیغامات بھیجے۔

کافی فعالیت: موبائل آلات تیزی سے دفتری فعالیت سے لیس ہوتے جارہے ہیں اور پہلے سے ہی اہم ڈیٹا اور ایپلی کیشنز لے جاتے ہیں، جو اکثر ناکافی طور پر محفوظ ہوتے ہیں یا بالکل بھی نہیں۔ توسیع شدہ فعالیت میلویئر کے امکان کو بھی بڑھاتی ہے۔

کافی رابطہ: اسمارٹ فونز متعدد مواصلاتی اختیارات پیش کرتے ہیں، جیسے کہ SMS، MMS، ہم آہنگی، بلوٹوتھ، انفراریڈ (IR) اور WLAN کنکشن۔ لہذا، بدقسمتی سے، آزادی کی بڑھتی ہوئی مقدار بھی وائرس لکھنے والوں کے لیے مزید انتخاب پیش کرتی ہے۔

موبائل-وائرس

مشنگ کا تصور

وشنگ کا تصور

مسکراہٹ کا تصور

ہیکنگ-بلوٹوتھ

5.7 موبائل کمپیوٹنگ کے دور میں تنظیمی سیکورٹی کی پالیسیاں اور اقدامات

استعمال شدہ ہاتھ سے پکڑے گئے آلات کا پھیلاؤ سائبر سیکیورٹی (Cyber security) کے مسئلے کو اس سے کہیں زیادہ سنگین بنا دیتا ہے جو ہم سوچتے ہیں۔ لوگ اپنے ہاتھ میں پکڑنے کے اتنے عادی ہو چکے ہیں کہ وہ ان کے ساتھ بٹوے کی طرح سلوک کر رہے ہیں! مثال کے طور پر، لوگ موبائل کمپیوٹنگ آلات پر ان کے آجروں یا وہ خود جانتے ہیں کے مقابلے میں زیادہ قسم کی خفیہ معلومات محفوظ کر رہے ہیں۔ وہ اپنے ہاتھ سے پکڑے گئے آلات کا استعمال کرتے ہوئے موسیقی سنتے ہیں۔ کسی کو سوچنا چاہیے کہ کریڈٹ کارڈ اور بینک اکاؤنٹ نمبر، پاس ورڈ، خفیہ ای میلز اور تنظیم، انضمام یا ٹیک اوور کے منصوبوں کے بارے میں اسٹریٹجک معلومات اور دیگر قیمتی معلومات بھی نہ رکھیں جو متاثر ہو سکتی ہیں۔ موبائل آلات میں اسٹاک کی قیمتیں کاروباری اثرات کا تصور کریں اگر کسی ملازم کی USB، پلگ ایبل ڈرائیو یا لیپ ٹاپ گم ہو یا چوری ہو جائے، جس سے کسٹمر کا حساس ڈیٹا جیسے کہ کریڈٹ رپورٹس، سوشل سیکیورٹی نمبرز (SSNs) اور رابطہ کی معلومات ظاہر ہو جائیں۔

موبائل ڈیوائس سیکیورٹی پالیسیوں کو نافذ کرنے کے لیے آپریٹنگ گائیڈ لائنز

اوپر بیان کردہ حالات میں، مثالی حل یہ ہوگا کہ تمام خفیہ ڈیٹا کو موبائل آلات پر ذخیرہ کرنے سے روکا جائے، لیکن یہ ہمیشہ عملی نہیں

ہو سکتا ہے۔ تاہم، تنظیمیں اس خطرے کو کم کر سکتی ہیں کہ درج ذیل اقدامات کے ذریعے گمشدہ یا چوری شدہ موبائل آلات سے خفیہ معلومات تک رسائی حاصل کی جائے گی۔

تنظیم، صنعت اور ریگولیٹری ماحول میں ان کے خطرات اور فوائد کی بنیاد پر اس بات کا تعین کریں کہ آیا تنظیم میں ملازمین کو موبائل کمپیوٹنگ ڈیوائسز کو بالکل بھی استعمال کرنے کی ضرورت ہے۔

اضافی سیکیورٹی ٹیکنالوجیز کو لاگو کریں، جیسا کہ تنظیم اور استعمال شدہ آلات کی اقسام دونوں کے لیے موزوں ہے۔ زیادہ تر (اور شاید سبھی) موبائل کمپیوٹنگ ڈیوائسز کو مضبوط انکرپشن، ڈیوائس پاس ورڈز اور فزیکل لاک جیسے ٹولز کے ساتھ اپنی مقامی سیکیورٹی کو بڑھانا ہوگا۔ بائیو میٹرکس تکنیک کے لیے استعمال کیا جا سکتا ہے۔ تصدیق اور خفیہ کاری اور پاس ورڈز سے وابستہ چیلنجوں کو ختم کرنے کی بڑی صلاحیت ہے۔

موبائل کمپیوٹنگ ڈیوائسز اور ان کے ساتھ استعمال کیے جانے والے متعلقہ سیکیورٹی ٹولز کو معیاری بنائیں۔ بنیادی اصول کے طور پر، سیکورٹی تیزی سے بگڑ جاتی ہے کیونکہ استعمال ہونے والے ٹولز اور آلات تیزی سے مختلف ہوتے جاتے ہیں۔

موبائل کمپیوٹنگ آلات کے استعمال کے لیے ایک مخصوص فریم ورک تیار کریں، بشمول ڈیٹا کی مطابقت پذیری کے لیے رہنما خطوط، فائروالز اور اینٹی میلویئر سافٹ ویئر کا استعمال اور ان معلومات کی اقسام جو ان پر محفوظ کی جا سکتی ہیں۔

اپنے موبائل کمپیوٹنگ آلات کے انتظام کو مرکزی بنائیں۔ انوینٹری کو برقرار رکھیں تاکہ آپ کو معلوم ہو کہ کون کس قسم کے آلات استعمال کر رہا ہے۔

موبائل آلات پر سافٹ ویئر کے لیے پیچنگ کے طریقہ کار کو قائم کریں۔ اسے اکثر مطابقت پذیری کے ساتھ پیچنگ کو مربوط کر کے یا مرکزی کے ساتھ پیچ کے انتظام کے ذریعے آسان بنایا جا سکتا ہے۔

موبائل آلات استعمال کرنے والے اہلکاروں کو تعلیم اور آگاہی کی تربیت فراہم کریں۔ لوگوں سے توقع نہیں کی جا سکتی کہ وہ اپنی معلومات کو مناسب طریقے سے محفوظ کر لیں اگر انہیں یہ نہیں بتایا گیا کہ کیسے۔

موبائل ہینڈ ہیلڈ ڈیوائسز کے استعمال کے لیے تنظیمی پالیسیاں

موبائل آلات کے لیے پالیسی بنانے کے معاملے کو سنبھالنے کے بہت سے طریقے ہیں۔ ایک طریقہ الگ موبائل کمپیوٹنگ پالیسی بنانا ہے۔ ایک اور طریقہ یہ ہے کہ اس طرح کے آلات کی موجودہ پالیسی بھی شامل ہے۔ اس کے درمیان ایسے نقطہ نظر بھی ہیں جہاں موبائل ڈیوائسز موجودہ پالیسیوں اور ایک نئی دونوں کے تحت آتے ہیں۔ ہائبرڈ اپروچ میں، موبائل ڈیوائسز کی مخصوص ضروریات کو پورا کرنے کے لیے ایک نئی پالیسی بنائی جاتی ہے لیکن عام استعمال کے مسائل عام IT پالیسیوں کے تحت آتے ہیں۔ اس نقطہ نظر کے ایک حصے کے طور پر، دیگر ٹیکنالوجیز کے لیے "قابل قبول استعمال" کی پالیسی کو موبائل آلات تک بڑھا دیا گیا ہے۔

موبائل آلات پر نئی کمپنیاں ایک چھتری والی موبائل پالیسی اپنا سکتی ہیں لیکن انہیں وقت گزرنے کے ساتھ ساتھ مختلف قسم کے موبائل ہینڈ ہیلڈ ڈیوائسز سے درپیش چیلنجوں سے نمٹنے کے لیے اپنی پالیسیوں میں ترمیم کرنے کی ضرورت ہوگی۔ مثال کے طور پر، وائرلیس

آلات غیر وائرلیس کے مقابلے میں مختلف چیلنجز پیش کرتے ہیں اس کے علاوہ، وہ ملازمین جو موبائل آلات کا 20%% سے زیادہ وقت استعمال کرتے ہیں ان کی ضروریات کم بار بار آنے والے صارفین سے مختلف ہوں گی۔ ایسا ہو سکتا ہے کہ وقت گزرنے کے ساتھ ساتھ، کمپنیوں کو موبائل آلات کے لیے اس بنیاد پر الگ پالیسیاں بنانے کی ضرورت پڑ سکتی ہے کہ آیا وہ وائرلیس طریقے سے جڑتے ہیں اور WANsاور LANsسے جڑنے والے آلات کے لیے امتیازات کے ساتھ۔

لیپ ٹاپ کا تصور:

جیسا کہ کمپیوٹنگ ٹیکنالوجی کی قیمت مسلسل کم ہو رہی ہے، لیپ ٹاپ جیسے آلات کا استعمال عام ہوتا جا رہا ہے۔ اگرچہ لیپ ٹاپ، دیگر موبائل آلات کی طرح، کسی بھی وقت اور کہیں بھی معلومات تک اپنے موبائل کی رسائی کی وجہ سے کاروباری افعال کو بڑھاتے ہیں، لیکن یہ ایک بڑا خطرہ بھی لاحق ہیں کیونکہ ان آلات میں پورٹیبل وائرلیس صلاحیت نے معلومات کی منتقلی کی وجہ سے سائبر سیکیورٹی(Cyber security) کے خدشات کو بھی جنم دیا ہے۔ دوسرے پر، جس کا پتہ لگانا مشکل ہو جاتا ہے۔

سائبر سیکیورٹی(Cyber security)انڈسٹری اور انشورنس کمپنی کے اعداد و شمار کے مطابق لیپ ٹاپ کی چوری ہمیشہ سے ایک بڑا مسئلہ رہا ہے۔ سائبر کرائمین مہنگے لیپ ٹاپ کو نشانہ بنا رہے ہیں، تاکہ وہ بلیک مارکیٹ میں فوری منافع حاصل کر سکیں۔ بہت کم لیپ ٹاپ۔ چور دراصل لیپ ٹاپ میں موجود معلومات میں دلچسپی رکھتے ہیں۔ زیادہ تر لیپ ٹاپ میں ذاتی اور کارپوریٹ معلومات ہوتی ہیں جو حساس ہو سکتی ہیں۔

جسمانی تحفظ کے انسداد کے اقدامات

تنظیمیں معلومات تک رسائی کے ساتھ موبائل ورک فورس پر بہت زیادہ انحصار کرتی ہیں، چاہے وہ کہیں بھی سفر کریں۔ تاہم، یہ نقل و حرکت تنظیموں کو ڈیٹا کی خلاف ورزی کے خطرے میں ڈال رہی ہے اگر حساس معلومات پر مشتمل لیپ ٹاپ گم ہو یا چوری ہو جائے۔ لہذا، جسمانی ملازمین کے لیپ ٹاپ پر معلومات کی حفاظت اور ملازمین کے لیپ ٹاپ سے محروم ہونے کے امکان کو کم کرنے کے لیے حفاظتی انسدادی اقدامات بہت اہم ہوتے جا رہے ہیں۔

کیبلز اور ہارڈ وائرڈ تالےCables and hardwired locks: کسی بھی موبائل ڈیوائس کی حفاظت کا سب سے سستا اور مثالی حل کیبلز اور تالے کے ساتھ محفوظ کرنا ہے، خاص طور پر لیپ ٹاپ کے لیے ڈیزائن کیا گیا ہے۔ کنسنگٹن کیبلز لیپ ٹاپ سیکیورٹی کیبل میں سب سے مشہور برانڈز میں سے ایک ہیں۔ یہ کیبلز ہوائی جہاز کے درجے کے اسٹیل اور کیولر برانڈ کے فائبر سے بنی ہیں، اس طرح یہ کیبلز کسی بھی دیگر روایتی حفاظتی کیبلز سے 40%% زیادہ مضبوط ہیں۔ سیکیورٹی کیبل کا ایک سرا لیپ ٹاپ کے یونیورسل سیکیورٹی سلاٹ میں فٹ ہوتا ہے اور دوسرا سرا کسی بھی مقررہ فرنیچر یا آئٹم کے گرد بند ہوتا ہے، اس طرح ایک لوپ بنتا ہے۔ یہ کیبلز متعدد اختیارات کے ساتھ آتی ہیں جیسے نمبر لاک، کلیدی تالے اور الارم۔

لیپ ٹاپ سیف: پولی کاربونیٹ سے بنے سیفز- وہی مواد جو بلٹ پروف کھڑکیوں، پولیس کے فسادات کی شیلڈز اور بینک سیکیورٹی اسکرینوں میں استعمال ہوتا ہے- لیپ ٹاپ کو لے جانے اور ان کی حفاظت کے لیے استعمال کیا جا سکتا ہے۔ سیکیورٹی کیبلز پر سیف کا فائدہ یہ ہے کہ وہ

پورے لیپ ٹاپ اور اس کے آلات جیسے CD-ROM بے ز، PCMCIA کارڈز اور HDD بے کی حفاظت کرتے ہیں جنہیں سیکیورٹی کیبلز کے ذریعے محفوظ لیپ ٹاپ کی صورت میں آسانی سے ہٹایا جاسکتا ہے۔

موشن سینسر زاور الارم: اگرچہ الارم اور موشن سینسر زاپنے غلط الارم اور بلند آواز کی سطح کی وجہ سے پریشان کن ہیں، یہ آلات لیپ ٹاپ کو محفوظ کرنے میں بہت کارآمد ہیں۔ ایک بار جب یہ ڈیوائسز ایکٹیویٹ ہو جائیں تو ان کا استعمال پر ہجوم جگہوں پر گمشدہ لیپ ٹاپس کو ٹریک کرنے کے لیے کیا جاسکتا ہے۔ نیز اپنی بلند طبیعت کی وجہ سے، وہ چوروں کو روکنے میں مدد کرتے ہیں۔ لیپ ٹاپ کے لیے جدید سسٹمز ڈیزائن کیے گئے ہیں جس میں لیپ ٹاپ سے منسلک الارم ڈیوائس لیپ ٹاپ کے ارد گرد ایک خاص حد تک ریڈیو سگنلز منتقل کرتی ہے۔

Warning labels and stamps: انتباہی لیبل جس میں ٹریکنگ کی معلومات اور شناخت کی تفصیلات شامل ہوں، لیپ ٹاپ پر فکس کیے جاسکتے ہیں تاکہ چوروں کو روکا جاسکے۔ یہ لیبل آسانی سے نہیں ہٹائے جاسکتے ہیں اور یہ لیپ ٹاپ کی چوری کا کم لاگت حل ہیں۔ ان لیبلز میں ایک شناختی نمبر ہوتا ہے جو تصدیق کے لیے یونیورسل ڈیٹا بیس میں محفوظ ہوتا ہے، جس کے نتیجے میں چوری شدہ لیپ ٹاپ کی دوبارہ فروخت ایک مشکل عمل بن جاتی ہے۔ تنظیموں کے اعلیٰ عہدیداروں اور/یا کلیدی ملازمین کو جاری کیے گئے لیپ ٹاپس کے لیے ایسے لیبلز کی انتہائی سفارش کی جاتی ہے۔

لیپ ٹاپ کی حفاظت کے لیے دیگر اقدامات درج ذیل ہیں۔

- لیپ ٹاپ کو ذاتی تفصیلات کے ساتھ کندہ کرنا
- جہاں تک ممکن ہو لیپ ٹاپ کو اپنے قریب رکھنا
- لیپ ٹاپ کو ایک مختلف اور غیر واضح بیگ میں لے جانا ممکنہ چوروں کے لیے غیر واضح ہو جاتا ہے۔
- لیپ ٹاپ لے جانے کی ذمہ داری اور لیپ ٹاپ میں موجود معلومات کی حساسیت کو سمجھنے کے لیے ملازمین میں بیداری پیدا کرنا۔
- خریداری کی رسید، لیپ ٹاپ سیریل نمبر اور لیپ ٹاپ کی تفصیل کی ایک کاپی بنانا
- لیپ ٹاپ پر محفوظ معلومات کی حفاظت کے لیے انکرپشن سافٹ ویئر انسٹال کرنا
- ناپسندیدہ رسائی اور مداخلت کو روکنے کے لیے ذاتی فائروال سافٹ ویئر کا استعمال
- اینٹی وائرس سافٹ ویئر کو باقاعدگی سے اپ ڈیٹ کرنا
- سیکیورٹی گارڈز کا استعمال کرتے ہوئے دفتر کی سخت حفاظت اور استعمال میں نہ ہونے پر لیپ ٹاپ کو لاکرز میں بند کر کے محفوظ کرنا

لیپ ٹاپ کو عوامی مقامات جیسے کار، پارکنگ لاٹ، کنونشنز، کانفرنسوں اور ہوائی اڈے پر اس وقت تک نہ چھوڑیں جب تک کہ اس میں چوری کے خلاف آلہ نصب نہ ہو۔

IR پورٹس اور وائرلیس کارڈز کو غیر فعال کرنا اور استعمال میں نہ ہونے پر PCMCIA کارڈز کو ہٹانا۔ انفارمیشن سسٹم سیکیورٹی میں منطقی رسائی کے کنٹرول بھی ہوتے ہیں۔ اس کی وجہ یہ ہے کہ معلومات، خواہ وہ کارپوریٹ ہو یا نجی، اسے اعلیٰ تحفظ کی ضرورت ہوتی ہے کیونکہ یہ کسی ادارے یا فرد کا سب سے اہم اثاثہ ہے۔ کچھ منطقی یا رسائی کے کنٹرول مندرجہ ذیل ہیں:

- بدنیتی پر مبنی پروگراموں/حملہ آوروں/سوشل انجینئرنگ سے تحفظ۔
- کمزور پاس ورڈز/رسائی سے گریز کرنا۔
- ایپلیکیشن سیکیورٹی کی نگرانی اور کمزوریوں کے لیے اسکیننگ۔
- اس بات کو یقینی بنانا کہ غیر خفیہ کردہ ڈیٹا/غیر محفوظ فائل سسٹمز خطرات کا باعث نہ ہوں۔
- ہٹانے کے قابل ڈرائیوز/اسٹوریج میڈیم/غیر ضروری پورٹس کی مناسب حوالے۔
- پاس ورڈ کی حفاظت مناسب پاس ورڈز کے قواعد اور مضبوط پاس ورڈ کے استعمال کے ذریعے۔
- ناپسندیدہ بندرگاہوں/آلات کو بند کرنا۔
- سیکیورٹی پیچ اور اپ ڈیٹس کو باقاعدگی سے انسٹال کرنا۔
- اینٹی وائرس سافٹ ویئر/فائروال/انٹروژن ڈیٹیکشن سسٹم (IDSs) انسٹال کرنا۔
- اہم فائل سسٹم کو خفیہ کرنا۔

5.10 اکتسابی نتائج

- موبائل اور وائرلیس کمپیوٹنگ کے بنیادی تصورات بیان کر سکے گا۔
- مختلف موبائل آلات جیسے Tablet PC، PDA، Smartphone اور Ultra Mobile PC کی وضاحت کر سکے گا۔
- موبائل اور وائرلیس کمپیوٹنگ میں کریڈٹ کارڈ فراڈ کے خطرات کو سمجھ سکے گا۔
- موبائل آلات کو درپیش Micro اور Macro Security Challenges بیان کر سکے گا۔
- موبائل آلات کی Registry Settings اور Authentication Service Security کی وضاحت کر سکے گا۔
- موبائل فونز پر ہونے والے مختلف حملوں کی شناخت کر سکے گا۔
- Malware، Virus، Worm، DoS، Overbilling اور Signaling-level Attacks کی وضاحت کر سکے گا۔
- موبائل ڈیوائس سیکیورٹی پالیسیوں کی اہمیت بیان کر سکے گا۔

5.11 کلیدی الفاظ

- موبائل کمپیوٹنگ Mobile Computing —

- وائرلیس کمپیوٹنگ — Wireless Computing
- موبائل ڈیوائس — Mobile Device
- اسمارٹ فون — Smartphone
- PDA — Personal Digital Assistant
- ٹیبلٹ پی سی — Tablet PC
- انٹرنیٹ ٹیبلٹ — Internet Tablet
- کریڈٹ کارڈ فراڈ — Credit Card Fraud
- موبائل بینکنگ — M-Banking
- موبائل کامرس — M-Commerce
- Malware
- Virus
- Worm
- Trojan

5.12 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1۔ موبائل کمپیوٹنگ کیا ہے؟

2۔ اسمارٹ فون کیا ہے؟

3۔ M-Commerce سے کیا مراد ہے؟

4۔ Malware کیا ہے؟

5۔ DoS Attack کیا ہے؟

مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1۔ موبائل کمپیوٹنگ اور وائرلیس کمپیوٹنگ کی وضاحت کریں۔

2۔ موبائل اور وائرلیس کمپیوٹنگ کے دور میں کریڈٹ کارڈ فراڈ کی وضاحت کریں۔

3۔ موبائل آلات کو درپیش مختلف سیکیورٹی چیلنجز بیان کریں۔

4۔ موبائل آلات کے لیے Registry Settings اور Authentication Service Security کی وضاحت کریں۔

5۔ موبائل فونز پر ہونے والے مختلف حملوں کی وضاحت کریں۔

6۔ Malware، Virus، Worm اور Trojan Attacks کی وضاحت کریں۔

7۔ DoS، DDoS اور Overbilling Attacks کی وضاحت کریں۔

8۔ موبائل کمپیوٹنگ کے دور میں تنظیمی سیکیورٹی پالیسیوں اور حفاظتی اقدامات کی وضاحت کریں۔

طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1۔ موبائل اور وائرلیس کمپیوٹنگ کی وضاحت کرتے ہوئے موبائل آلات کی مختلف اقسام، ان کے استعمال اور ان سے متعلق سیکیورٹی خطرات کی تفصیل سے وضاحت کریں۔

2۔ موبائل فونز اور موبائل نیٹ ورکس پر ہونے والے مختلف سائبر حملوں کی تفصیل سے وضاحت کریں۔ Malware، Virus، Worm، Trojan، DoS، DDoS، Overbilling اور Signaling-level Attacks کو بیان کریں۔

3۔ موبائل کمپیوٹنگ کے دور میں تنظیمی سیکیورٹی پالیسیوں اور اقدامات کی تفصیل سے وضاحت کریں۔ موبائل ڈیوائسز اور لیپ ٹاپ کی حفاظت کے لیے Encryption، Passwords، Firewall، Antivirus، Physical Locks، Patching اور Security Awareness کی اہمیت بیان کریں۔

5.13 تجویز کردہ اکتسابی مواد

1۔ موبائل اور وائرلیس کمپیوٹنگ کا تعارف

2۔ موبائل آلات اور ان کی اقسام

3۔ موبائل اور وائرلیس کمپیوٹنگ میں کریڈٹ کارڈ فراڈ

4۔ موبائل آلات کے سیکیورٹی چیلنجز

5۔ موبائل آلات کی Registry Settings

6۔ Authentication Service Security

7۔ موبائل فونز پر مختلف Cyber Attacks

8۔ Malware، Viruses، Worms اور Trojans

9۔ DoS اور DDoS Attacks

10۔ Overbilling Attack

11۔ Spoofed PDP اور Signaling-level Attacks

12۔ موبائل ڈیوائس سیکیورٹی پالیسیاں

13۔ لیپ ٹاپ کی Physical اور Logical Security

اکائی6۔ سائبر سیکیورٹی: تنظیمی اثرات

(Cyber Security: Organizational Implications)

اکائی کے اجزاء

6.0 تمہید

6.1 مقاصد

6.2 تنظیموں میں سائبر سیکیورٹی(Cyber security)کا تعارف

6.3 سائبر کرائمز اور انٹلیکچوئل پراپرٹی رائٹس(IPR)کے مسائل کی لاگت

6.4 تنظیموں کے لیے ویب دھمکیاں

6.5 تنظیموں میں سیکورٹی اور رازداری کے مضمرات

6.6 سوشل میڈیا مارکیٹنگ: تنظیموں کے لیے حفاظتی خطرات اور خطرات

6.7 تنظیموں کے لیے سماجی کمپیوٹنگ اور اس سے وابستہ چیلنجز

6.8 اکتسابی نتائج

6.9 کلیدی الفاظ

6.10 نمونہ امتحانی سوالات

6.11 تجویز کردہ اکتسابی مواد

6.0 تمہید

اس اکائی میں تنظیموں میں سائبر سیکیورٹی کی اہمیت، سائبر کرائم اور انٹلیکچوئل پراپرٹی رائٹس (IPR) کے مسائل، ویب پر مبنی خطرات، سیکیورٹی اور رازداری کے مضمرات، سوشل میڈیا مارکیٹنگ کے سیکیورٹی خطرات اور سماجی کمپیوٹنگ سے وابستہ چیلنجز کا مطالعہ کیا جاتا ہے۔

6.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- تنظیموں میں سائبر سیکیورٹی کے بنیادی تصورات کو سمجھ سکیں گے۔
- سائبر کرائم اور IPR کے مسائل اور ان کے اخراجات کی وضاحت کر سکیں گے۔
- تنظیموں کو درپیش مختلف ویب خطرات کی شناخت کر سکیں گے۔
- تنظیمی سیکیورٹی اور رازداری کے مضمرات کو سمجھ سکیں گے۔
- سوشل میڈیا مارکیٹنگ سے وابستہ سیکیورٹی خطرات کی وضاحت کر سکیں گے۔
- سماجی کمپیوٹنگ کے فوائد اور چیلنجز کو بیان کر سکیں گے۔

6.2 تنظیموں میں سائبر سیکیورٹی (Cyber security) کا تعارف

سائبر سیکورٹی کیا ہے؟

سائبر سیکیورٹی (Cyber security) سے مراد سسٹمز، نیٹ ورکس اور ڈیٹا کو سائبر خطرات (Cyber threats) سے بچانے کی مشق ہے۔ تنظیمیں اپنی حساس معلومات، املاک دانش اور مالیاتی ڈیٹا کی حفاظت کے لیے سائبر سیکیورٹی (Cyber security) پر انحصار کرتی ہیں۔

سائبر سیکیورٹی (Cyber security) اداروں کے لیے کیوں اہم ہے؟

- سائبر کرائمینلز سے کاروباری ڈیٹا کی حفاظت کرتا ہے۔
- سائبر فراڈ اور ڈیٹا کی خلاف ورزیوں کی وجہ سے ہونے والے مالی نقصانات کو روکتا ہے۔
- قانونی اور ریگولیٹری معیارات کی تعمیل کو یقینی بناتا ہے۔
- گاہک کے اعتماد اور برانڈ کی ساکھ کو برقرار رکھتا ہے۔
- اہم انفراسٹرکچر اور آپریشنز کو محفوظ بناتا ہے۔

سائبر سیکیورٹی (Cyber security) کے کلیدی تصورات

- رازداری: اس بات کو یقینی بنانا کہ صرف مجاز صارفین معلومات تک رسائی حاصل کر سکیں۔
- سالمیت: ڈیٹا کی غیر مجاز ترمیم کو روکنا۔
- دستیابی: اس بات کو یقینی بنانا کہ ضرورت پڑنے پر وسائل اور خدمات قابل رسائی ہوں۔

6.3 سائبر کرائمز اور انٹلیکچوئل پراپرٹی رائٹس (IPR) کے مسائل کی لاگت

سائبر کرائمز اور ان کے اخراجات کو سمجھنا

سائبر کرائمز میں ہیکنگ، فشنگ، رینسم ویئر کے (Attacks) اور ڈیٹا کی خلاف ورزی جیسی سرگرمیاں شامل ہیں۔ یہ جرائم پیسے،

وقت اور شہرت کے لحاظ سے تنظیموں پر بھاری قیمتیں عائد کرتے ہیں۔

سائبر کرائمز کے مالیاتی اثرات

- کاروبار میں خلل کی وجہ سے آمدنی کا نقصان۔
- ریگولیٹری جرمانے اور قانونی اخراجات۔
- کمپرومائزڈ سسٹمز اور ڈیٹا کی بازیابی کی لاگت۔
- متاثرہ صارفین کے لیے معاوضہ۔

ساکھ کو پہنچنے والا نقصان

ایک سائبر حملہ کسٹمر کے اعتماد کو ختم کر سکتا ہے، جس سے کاروبار کو نقصان پہنچ سکتا ہے۔ڈیٹا کی خلاف ورزیوں کی وجہ سے بہت سی کمپنیوں کو بڑے دھچکے کا سامنا کرنا پڑا ہے (مثال کے طور پر، Yahoo،Equifax)۔

انٹلیکچوئل پراپرٹی رائٹس (IPR) اور سائبر سیکیورٹی (Cyber security)

- آئی پی چوری: سائبر کرائمین تجارتی راز، سافٹ ویئر کوڈز، یا پروڈکٹ ڈیزائن چراتے ہیں۔
- جعل سازی (**Counterfeiting**): چوری شدہ ڈیٹا کو جعلی مصنوعات بنانے کے لیے استعمال کیا جاتا ہے۔
- ڈیجیٹل پائریسی (**Digital Piracy**): سافٹ ویئر، فلموں یا کتابوں کی غیر مجاز کاپی اور تقسیم۔

سائبر اسپیس میں آئی پی آر کی حفاظت

- انکرپشن اور ڈیجیٹل رائٹس مینجمنٹ (DRM) کو نافذ کرنا۔
- غیر مجاز رسائی یا لیک کے لئے نگرانی.
- سائبر جرائم پیشہ افراد کے خلاف قانونی کارروائیوں کا نفاذ۔
- حساس IP کی حفاظت کے لیے سائبر سیکیورٹی (Cyber security) فریم ورک کا استعمال۔

6.4 تنظیموں کے لیے ویب دھمکیاں

عام ویب پر مبنی خطرات

- فشنگ attack (Attacks)phishing): دھوکہ دہی پر مبنی ای میلز یا ویب سائٹس ملازمین کو خفیہ ڈیٹا افشا کرنے کے لیے پھنساتی ہیں۔
- مالویئر (Attacks): نقصان دہ سافٹ ویئر سسٹم میں گھس کر ڈیٹا چوری کرتا ہے۔
- رینسم ویئر Ransomware): سائبر کرائمین کمپنی کے ڈیٹا کو خفیہ کرتے ہیں اور اس کی رہائی کے لیے ادائیگی کا مطالبہ کرتے ہیں۔

- DDoS (Attacks): کسی ویب سائٹ یا سروس کو ٹریفک کے ساتھ اوورلوڈ کرنا، جس سے ڈاؤن ٹائم ہوتا ہے۔
- ایس کیو ایل انجیکشن اور ایکس ایس ایس ایسXSS Attacks & SQL Injection (Attacks)): غیر مجاز رسائی حاصل کرنے کے لیے ویب ایپلیکیشنز میں کمزوریوں کا فائدہ اٹھانا۔

تنظیموں پر ویب دھمکیوں (threat) (threat) کا اثر

- خفیہ کاروبار اور کسٹمر ڈیٹا کا نقصان۔
- ڈیٹا کی خلاف ورزیوں کی وجہ سے قانونی نتائج۔
- ڈاؤن ٹائم اور کاروبار میں خلل۔
- سائبر سیکیورٹی (Cyber security) کے اخراجات میں اضافہ۔

تخفیف کی حکمت عملی

- مضبوط فائر وال اور مداخلت کا پتہ لگانے کے نظام کو لاگو کریں۔
- سافٹ ویئر اور سیکیورٹی پیچ کو باقاعدگی سے اپ ڈیٹ کریں۔
- فشنگ کے خطرات کو پہچاننے کے لیے ملازمین کی تربیت کا انعقاد کریں۔
- محفوظ رسائی کے لیے ملٹی فیکٹر توثیق کا استعمال کریں۔

6.5 تنظیموں میں سیکورٹی اور رازداری کے مضمرات

تنظیمی ڈیٹا کے تحفظ کی حکمت عملی

- ڈیٹا کی خفیہ کاری Data Encryption: غیر مجاز رسائی کو روکنے کے لیے ڈیٹا کو انکوڈنگ کرنا۔
- رسائی کنٹرول Access Control: صارف کے کردار کی بنیاد پر حساس ڈیٹا تک رسائی کو محدود کرنا۔
- سیکورٹی پالیسیاں Security Policies: ڈیٹا ہینڈلنگ اور سسٹم تک رسائی کے قوانین کا قیام۔
- واقعہ رسپانس پلان Incident Response Plan): سیکیورٹی کی خلاف ورزیوں سے نمٹنے کے لیے پہلے سے طے شدہ طریقہ۔

تعمیل اور ریگولیٹری معیارات

قانونی نتائج سے بچنے کے لیے تنظیموں کو سائبر سیکیورٹی (Cyber security) کے ضوابط پر عمل کرنا چاہیے:

- GDPR (جنرل ڈیٹا پروٹیکشن ریگولیشن)- یورپی یونین کے شہریوں کے ڈیٹا کی حفاظت کرتا ہے۔
- HIPAA (ہیلتھ انشورنس پورٹیبلٹی اور احتساب ایکٹ)- صحت کی دیکھ بھال کی معلومات کی حفاظت کو یقینی بناتا ہے۔
- ISO/IEC 27001- انفارمیشن سیکیورٹی مینجمنٹ کے لیے بین الاقوامی معیار۔

اندرونی خطرات اور رسک مینجمنٹ

- ملازمین یا ٹھیکیدار جان بوجھ کر یا غیر ارادی طور پر سیکورٹی کے خطرات کا باعث بن سکتے ہیں۔
- رسائی کی سخت پالیسیوں کو نافذ کرنا اور ملازمین کی سرگرمیوں کی نگرانی خطرات کو کم کر سکتی ہے۔
- ملازمین کے لیے باقاعدہ آڈٹ اور پس منظر کی جانچ کرنا۔

6.6 سوشل میڈیا مارکیٹنگ: تنظیموں کے لیے حفاظتی خطرات اور خطرات

تنظیموں میں سوشل میڈیا کا استعمال کیسے کیا جاتا ہے۔

- برانڈ پروموشن اور مارکیٹنگ مہمات۔
- گاہک کی مصروفیت اور آراء جمع کرنا۔
- بھرتی اور کاروباری نیٹ ورکنگ۔

سوشل میڈیا مارکیٹنگ میں سیکورٹی کے خطرات

- شناخت کی چوری اور نقالیIdentity Theft & Impersonation: ہیکرز صارفین کو دھوکہ دینے کے لیے جعلی پروفائل بناتے ہیں۔
- فشنگ سکیمز: حملہ آور سوشل میڈیا کے ذریعے بدنیتی پر مبنی لنک بھیجتے ہیں۔
- ڈیٹا لیکس: ملازمین غلطی سے خفیہ معلومات کا اشتراک کرتے ہیں۔
- شہرت کے خطرات: منفی تبصرے یا ہیک شدہ اکاؤنٹس برانڈ امیج کو نقصان پہنچا سکتے ہیں۔

تخفیف کی حکمت عملی

- مضبوط پاس ورڈ استعمال کریں اور دو عنصر کی توثیق کو فعال کریں۔
- ملازمین کو سوشل میڈیا کے خطرات سے آگاہ کریں۔
- مشکوک سرگرمی کے لیے کمپنی کے سوشل میڈیا اکاؤنٹس کی نگرانی کریں۔
- سرکاری سوشل میڈیا اکاؤنٹس تک رسائی کو قابل اعتماد اہلکاروں تک محدود کریں۔

6.7 تنظیموں کے لیے سماجی کمپیوٹنگ اور اس سے وابستہ چیلنجز

سوشل کمپیوٹنگ کیا ہے؟

سوشل کمپیوٹنگ سے مراد ڈیجیٹل پلیٹ فارمز کا استعمال ہے جو سماجی تعاملات کو آسان بناتے ہیں، جیسے کہ سوشل نیٹ ورکس، اشتراکی ٹولز، اور کلاؤڈ بیسڈ ایپلی کیشنز۔

تنظیموں میں سوشل کمپیوٹنگ کے فوائد

- مواصلات اور تعاون کو بہتر بناتا ہے۔
- علم کے اشتراک اور جدت کو بڑھاتا ہے۔
- ملازمین کی مصروفیت کو بڑھاتا ہے۔

چیلنجز اور خطرات

- حفاظتی خطرات: حساس کاروباری معلومات غیر مجاز جماعتوں کے سامنے آسکتی ہیں۔
- رسائی کنٹرول کے مسائل Access Control Issues: مشترکہ پلیٹ فارمز تک رسائی کا انتظام کرنا مشکل ہے۔
- تعمیل اور قانونی خدشات Compliance and Legal Concerns: ڈیٹا کے تحفظ کے قوانین پر عمل کرنا ضروری ہے۔
- سائبر دھونس اور اخلاقی خدشات Cyberbullying and Ethical Concerns: سماجی پلیٹ فارم کا غلط استعمال کام کی جگہ پر تنازعات کا باعث بن سکتا ہے۔

محفوظ سوشل کمپیوٹنگ کے لیے بہترین طریقے

- اشتراکی پلیٹ فارمز کے لیے سخت رسائی کے کنٹرول کو نافذ کریں۔
- ملازمین کے لیے سیکیورٹی سے متعلق آگاہی کی باقاعدہ تربیت کا انعقاد کریں۔
- سوشل کمپیوٹنگ ٹولز کے استعمال پر واضح پالیسیاں بنائیں۔
- سماجی پلیٹ فارمز پر اشتراک کردہ حساس مواصلات اور ڈیٹا کو خفیہ کریں۔

6.8 اکتسابی نتائج

- تنظیموں میں سائبر سیکیورٹی کی اہمیت بیان کر سکیں گے۔
- سائبر جرائم اور IPR کے مسائل کے مالی و ساکھ پر اثرات سمجھ سکیں گے۔
- تنظیموں کو درپیش ویب دھمکیوں کی شناخت کر سکیں گے۔
- سیکیورٹی اور رازداری کے مضمرات بیان کر سکیں گے۔
- سوشل میڈیا مارکیٹنگ کے سیکیورٹی خطرات سمجھ سکیں گے۔
- سماجی کمپیوٹنگ کے فوائد اور چیلنجز بیان کر سکیں گے۔

6.9 کلیدی الفاظ

- Cybercrime
- IPR
- Web Threats
- Phishing
- Malware
- Ransomware
- DDoS
- SQL Injection
- XSS
- Data Encryption
- Access Control
- Security Policies
- GDPR
- HIPAA
- ISO/IEC 27001

6.10 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1۔ سائبر سیکیورٹی سے کیا مراد ہے؟

2۔ IPR کی مکمل شکل کیا ہے؟

3۔ فشنگ (Phishing) کیا ہے؟

4۔ DDoS کی مکمل شکل کیا ہے؟

5۔ Social Computing سے کیا مراد ہے؟

مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1۔ تنظیموں میں سائبر سیکیورٹی کی اہمیت بیان کریں۔

2۔ سائبر کرائمز کے تنظیموں پر مالیاتی اثرات بیان کریں۔

3۔ سائبر سیکیورٹی میں IPR کے مسائل کی وضاحت کریں۔

4۔ تنظیموں کو درپیش مختلف ویب دھمکیوں کی وضاحت کریں۔

5۔ تنظیموں میں سیکیورٹی اور رازداری کے مضمرات بیان کریں۔

6۔ سوشل میڈیا مارکیٹنگ کے سیکیورٹی خطرات بیان کریں۔

7۔ Social Computing کے فوائد اور چیلنجز بیان کریں۔

8۔ تنظیموں میں سائبر سیکیورٹی کے خطرات کو کم کرنے کے طریقے بیان کریں۔

طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1۔ تنظیموں کے لیے ویب دھمکیوں، ان کے اثرات اور حفاظتی اقدامات کی تفصیل بیان کریں۔

2۔ سائبر کرائمز اور IPR کے مسائل کی تنظیموں پر لاگت اور اثرات کی وضاحت کریں۔

3۔ Social Media Marketing اور Social Computing کے فوائد، خطرات اور حفاظتی اقدامات تفصیل سے بیان کریں۔

6.11 تجویز کردہ اکتسابی مواد

1۔ Cybercrime اور اس کے مالی اثرات

2۔ Intellectual Property Rights (IPR)

3۔ Web Threats

4۔ Data Privacy اور Security

5۔ Social Media Security

6۔ Social Computing

7۔ Access Control

8۔ Data Encryption

9۔ Phishing، Malware، Ransomware اور DDoS

10۔ GDPR، HIPAA اور ISO/IEC 27001

11۔ Cyber Security Best Practices

اکائی 7۔ رازداری کے مسائل اور سائبر کرائم

(Privacy Issues and Cybercrime)

اکائی کے اجزاء

7.0 تمہید

7.1 مقاصد

7.2 ڈیٹاپرائیویسی کا تعارف

7.3 ڈیٹاپرائیویسی کے بنیادی تصورات Fundamental Concepts of Data Privacy

7.4 ڈیٹاپرائیویسی (Attacks)

7.5 ڈیٹا لنکنگ اور پروفائلنگ Data Linking and Profiling

7.6 رازداری کی پالیسیاں اور ان کی تفصیلات Privacy Policies and Their Specifications

7.7 رازداری کی پالیسی کی زبانیں۔ Privacy Policy Languages

7.8 مختلف ڈومینز میں رازداری

7.9 ہندوستان میں سائبر کرائم پر چھوٹے کیسز

7.10 اکتسابی نتائج

7.11 کلیدی الفاظ

7.12 نمونہ امتحانی سوالات

7.13 تجویز کردہ اکتسابی مواد

7.0 تمہید

آج کی ڈیجیٹل دنیا میں ڈیٹاپرائیویسی ایک اہم مسئلہ ہے۔ ذاتی اور حساس ڈیٹا کی بڑھتی ہوئی مقدار کے باعث اسے غلط استعمال، سائبر حملوں اور غیر مجاز رسائی سے محفوظ رکھنا ضروری ہے۔ اس اکائی میں ڈیٹاپرائیویسی کے بنیادی تصورات، پرائیویسی حملوں، ڈیٹا لنکنگ اور پروفائلنگ، رازداری کی پالیسیوں، مختلف ڈومینز میں رازداری اور ہندوستان میں سائبر کرائم کے چھوٹے کیسز کا مطالعہ کیا جائے گا۔

7.1 مقاصد

اس اکائی کے مطالعہ کے بعد آپ:

- ڈیٹا پرائیویسی کے بنیادی تصورات کو سمجھ سکیں گے۔
- ڈیٹا پرائیویسی کے مختلف حملوں کی شناخت اور وضاحت کر سکیں گے۔
- ڈیٹا لنکنگ اور پروفائلنگ کو سمجھ سکیں گے۔
- رازداری کی پالیسیوں اور ان کی خصوصیات کو بیان کر سکیں گے۔

7.2 ڈیٹا پرائیویسی کا تعارف

ڈیٹا پرائیویسی آج کی ڈیجیٹل دنیا میں سب سے اہم خدشات میں سے ایک ہے۔ آن لائن ذخیرہ شدہ ذاتی اور حساس ڈیٹا کی بڑھتی ہوئی مقدار کے ساتھ، اسے غلط استعمال اور غیر مجاز رسائی سے بچانا ضروری ہو گیا ہے۔ حکومتیں، کارپوریشنز، اور افراد سبھی ڈیٹا کی رازداری کو برقرار رکھنے کو یقینی بنانے میں اپنا کردار ادا کرتے ہیں۔

7.3 ڈیٹا پرائیویسی کے بنیادی تصورات (Fundamental Concepts of Data Privacy)

ڈیٹا کی رازداری تین اہم اصولوں کے گرد گھومتی ہے:

- رازداری confidentiality: اس بات کو یقینی بنانا کہ ذاتی ڈیٹا تک رسائی صرف مجاز افراد کے ذریعہ ہو۔
- سالمیت Integrity: ڈیٹا کی درستگی اور اعتماد کو برقرار رکھنا۔
- دستیابی Availability: اس بات کو یقینی بنانا کہ جب ضرورت ہو تو جائز صارفین تک ڈیٹا قابل رسائی رہے۔

ڈیٹا سے چلنے والی ٹیکنالوجیز کے عروج کے ساتھ، تنظیموں کو صارف کی معلومات کو خلاف ورزیوں، غیر مجاز رسائی اور استحصال سے بچانے کے لیے رازداری کے مضبوط اقدامات کو اپنانا چاہیے۔

7.4 ڈیٹا پرائیویسی (Attacks)

سائبر جرائم پیشہ افراد اکثر مالی فائدہ، شناخت کی چوری، یا کارپوریٹ جاسوسی کے لیے ذاتی اور تنظیمی ڈیٹا کو نشانہ بناتے ہیں۔ کچھ عام ڈیٹا پرائیویسی حملوں میں شامل ہیں:

- فشنگ (Attacks): سائبر جرائم پیشہ افراد کو فریب دینے والی ای میلز یا ویب سائٹس کے ذریعے حساس ڈیٹا فراہم کرنے کے لیے دھوکہ دیتے ہیں۔
- میلویئر اور رینسم ویئر: نقصان دہ سافٹ ویئر اہم ڈیٹا چوری کرنے یا لاک کرنے کے لیے سسٹمز میں گھس جاتا ہے۔

- مین ان دی مڈل Man-in-the-Middle Attacks(Attacks): ہیکرز نجی ڈیٹا تک رسائی حاصل کرنے کے لیے دو فریقوں کے درمیان مواصلات کو روکتے ہیں۔
- اندرونی دھمکیاں Insider Threats: ملازمین یا شراکت دار جان بوجھ کر یا غلطی سے خفیہ ڈیٹا کو بے نقاب کرتے ہیں۔

یہ (Attacks) نہ صرف مالی نقصان کا باعث بنتے ہیں بلکہ ساکھ کو بھی نقصان پہنچاتے ہیں اور قانونی ضابطوں کی خلاف ورزی کرتے ہیں۔

7.5 ڈیٹا لنکنگ اور پروفائلنگ (Data Linking and Profiling)

ڈیٹا لنکنگ اور پروفائلنگ ڈیٹا پرائیویسی میں دو اہم خدشات ہیں۔

- ڈیٹا لنکنگ Data Linking: یہ تکنیک افراد کے بارے میں تفصیلی معلومات نکالنے کے لیے متعدد ڈیٹا سیٹس کو یکجا کرتی ہے۔ مثال کے طور پر، سوشل میڈیا کی سرگرمی کو مالی لین دین کے ساتھ جوڑنے سے اخراجات کے نمونوں اور طرز عمل کی بصیرت کا پتہ چل سکتا ہے۔
- پروفائلنگ: کمپنیاں اور حکومتیں افراد کے ڈیجیٹل پروفائلز ان کی آن لائن سرگرمیوں، خریداریوں اور ترجیحات کی بنیاد پر بناتی ہیں۔ اگرچہ اس سے ٹارگٹ ایڈورٹائزنگ اور خطرے کی تشخیص میں مدد ملتی ہے، لیکن یہ ڈیٹا کے رضامندی اور غلط استعمال کے حوالے سے اخلاقی خدشات کو جنم دیتا ہے۔

بڑے ڈیٹا سیٹس کو سنبھالتے وقت تنظیموں کو صارف کی شناخت کے تحفظ کے لیے مضبوط خفیہ کاری اور گمنامی کی تکنیکوں کو لاگو کرنا چاہیے۔

7.6 رازداری کی پالیسیاں اور ان کی تفصیلات (Privacy Policies and Their Specifications)

رازداری کی پالیسیاں اس بات کا خاکہ پیش کرتی ہیں کہ کس طرح ایک تنظیم صارف کے ڈیٹا کو اکٹھا کرتی ہے، اسٹور کرتی ہے اور اس پر کارروائی کرتی ہے۔ ایک اچھی طرح سے متعین رازداری کی پالیسی میں شامل ہونا چاہئے:

- کیا ڈیٹا اکٹھا کیا جاتا ہے اور کیوں۔
- ڈیٹا کو کیسے محفوظ اور محفوظ کیا جاتا ہے۔
- آیا ڈیٹا تیسرے فریق کے ساتھ شیئر کیا گیا ہے۔
- ڈیٹا تک رسائی، ترمیم، اور حذف کرنے سے متعلق صارف کے حقوق۔

کمپنیوں کو عالمی ضوابط جیسے کہ جنرل ڈیٹا پروٹیکشن ریگولیشن (GDPR) اور کیلیفورنیا کنزیومر پرائیویسی ایکٹ (CCPA) شفافیت اور صارف کے اعتماد کو یقینی بنانے کے لیے۔

7.7 رازداری کی پالیسی کی زبانیں(Privacy Policy Languages)

رازداری کی پالیسی کی زبانیں رازداری کے قوانین کی وضاحت اور نفاذ میں مدد کرتی ہیں۔ کچھ وسیع پیمانے پر استعمال ہونے والی زبانوں میں شامل ہیں:

- P3P(پرائیویسی ترجیحات کے لیے پلیٹ فارم): W3C کے ذریعہ تیار کردہ، یہ زبان ویب سائٹس کو مشین کے پڑھنے کے قابل فارمیٹ میں اپنی رازداری کی پالیسیوں کی وضاحت کرنے میں مدد کرتی ہے۔
- XACML(ایکسٹینسیبل ایکسیس کنٹرول مارک اپ لینگویج): حساس ڈیٹا کی حفاظت کے لیے رسائی کنٹرول پالیسیوں کی وضاحت کے لیے استعمال کیا جاتا ہے۔
- EPAL(انٹرپرائزپرائیویسی اتھارٹی کی زبان): تنظیموں کو ڈیٹاہینڈلنگ کے لیے رازداری کی پالیسیاں نافذ کرنے میں مدد کرتا ہے۔

ان زبانوں کو ڈیجیٹل سسٹمز میں ضم کرکے، تنظیمیں رازداری کے نفاذ کو خودکار کرسکتی ہیں اور تعمیل کو یقینی بناسکتی ہیں۔

7.8 مختلف ڈومینز میں رازداری

رازداری کے خدشات مختلف صنعتوں میں مختلف ہوتے ہیں۔

- میڈیکل سیکٹر: مریض کے ریکارڈ میں انتہائی حساس معلومات ہوتی ہیں۔ جیسے ضابطے۔ HIPAA (ہیلتھ انشورنس پورٹیبلٹی اور احتساب ایکٹ) یقینی بنائیں کہ طبّی ڈیٹا خفیہ اور محفوظ رہے۔
- مالیاتی شعبہ Financial Sector: بینک اور مالیاتی ادارے لین دین کے ڈیٹا کی بڑی مقدار کا انتظام کرتے ہیں۔ رازداری کے اقدامات میں ملٹی فیکٹر توثیق اور اینڈ ٹو اینڈ انکرپشن شامل ہیں۔
- ای کامرس اور ریٹیل E-commerce and Retail: صارفین کا ڈیٹا، بشمول خریداری کی تاریخ اور ذاتی ترجیحات، کو ڈیٹا کی خلاف ورزیوں اور غیر مجاز ٹریکنگ سے محفوظ رکھا جانا چاہیے۔
- ان ڈومینز میں ڈیٹا کی رازداری کو برقرار رکھنے کے لیے سیکیورٹی، استعمال کے قابل اور عالمی رازداری کے قوانین کی تعمیل کے درمیان توازن کی ضرورت ہوتی ہے۔

سیکشن2: سائبر کرائم–مثالیں اور چھوٹے کیسز Cybercrime –Examples and Mini-Cases

سائبر کرائم قومی سلامتی، کاروباری اداروں اور افراد کے لیے ایک بڑا خطرہ بن گیا ہے۔ ہندوستان نے کئی ہائی پروفائل سائبر کرائم کے واقعات دیکھے ہیں، جو ڈیجیٹل سسٹمز میں موجود کمزوریوں کو اجاگر کرتے ہیں۔

ہندوستان میں سائبر کرائمز کی مثالیں۔

1۔ مہاراشٹر حکومت کی ویب سائٹ ہیکنگ: اس واقعے میں مہاراشٹر حکومت کی آفیشل ویب سائٹ کو ہیک کرلیا گیا، جس کے نتیجے میں حساس

شہریوں کے ڈیٹا تک غیر مجاز رسائی ہوئی۔ ہیکرز نے ویب سائٹ کو خراب کیا اور خفیہ سرکاری معلومات چرالیں۔ اس کیس نے سرکاری پورٹلز میں مضبوط سائبر سیکیوریٹی اقدامات کی ضرورت کو اجاگر کیا۔

2۔ ہندوستانی بینکوں کو سائبر فراڈ سے لاکھوں کا نقصان ہوا۔: سائبر فراڈ جس میں فشنگ، اے ٹی ایم کارڈ کلوننگ، اور غیر مجاز لین دین شامل ہیں، کی وجہ سے کئی ہندوستانی بینکوں کو بڑے مالی نقصان کا سامنا کرنا پڑا۔ ایک انتہائی بدنام کیس میں ہیکرز کا بینکنگ سسٹم میں دراندازی کرنا اور لاکھوں کو جعلی اکاؤنٹس میں منتقل کرنا شامل ہے۔

3۔ پارلیمنٹ حملہ (سائبر پہلو)(The Parliament Attack (Cyber Aspect: 2001 میں ہندوستانی پارلیمنٹ پر بدنام زمانہ دہشت گردانہ (Attacks) کے دوران، ڈیجیٹل شواہد سے پتہ چلتا ہے کہ دہشت گرد مواصلات اور منصوبہ بندی کے لیے انٹرنیٹ کا استعمال کرتے تھے۔ اس کیس نے قومی سلامتی میں سائبر انٹیلی جنس کے کردار کو اجاگر کیا۔

4۔ پونے سٹی پولیس نے نائجیرین سائبر ریکیٹ کا پردہ فاش کیا :پونے پولیس نے نائجیریا کے دھوکہ بازوں کے ذریعہ چلائے جانے والے سائبر فراڈ نیٹ ورک کا پردہ فاش کیا۔ مجرموں نے جعلی لاٹری اسکیموں اور فشنگ ای میلز کا استعمال کرتے ہوئے متاثرین کو رقم کی منتقلی کے لیے دھوکہ دیا۔ اس کیس نے یہ ظاہر کیا کہ کس طرح بین الاقوامی سائبر کرائم نیٹ ورک ڈیجیٹل پلیٹ فارم کا استحصال کرتے ہیں۔

5۔ ہندوستان میں ای میل سپوفنگ کیسز :ای میل کی جعل سازی نے ہندوستان میں اہم دھوکہ دہی کا باعث بنی ہے، جہاں حملہ آور ایسی ای میلز بھیجتے ہیں جو بظاہر جائز تنظیموں سے ہوتے ہیں، اور صارفین کو حساس ڈیٹا شیئر کرنے کے لیے دھوکہ دیتے ہیں۔ یہ واقعات ای میل کی توثیق کے پروٹوکول کی اہمیت پر زور دیتے ہیں۔

7.9 ہندوستان میں سائبر کرائم پر چھوٹے کیسز

1۔ آن لائن جوئے کا ہندوستانی معاملہ: آن لائن جوئے کو ہندوستان میں مقبولیت حاصل ہوئی ہے، لیکن بہت سے پلیٹ فارم غیر قانونی طور پر کام کرتے ہیں۔ سائبر کرائمین منی لانڈرنگ اور دھوکہ دہی کے لیے ان پلیٹ فارمز کا استحصال کرتے ہیں۔ آن لائن لین دین کی گمنام نوعیت کی وجہ سے ریگولیٹری ادارے جوئے کی غیر قانونی سرگرمیوں کو کنٹرول کرنے کے لیے جدوجہد کر رہے ہیں۔

2۔ ہندوستان میں دانشورانہ املاک کا جرم: ہندوستان میں سافٹ ویئر کی بحری قزاقی اور جعلی مصنوعات کی فروخت کے متعدد واقعات دیکھنے میں آئے ہیں۔ ایک قابل ذکر کیس میں ایک کمپنی غیر قانونی طور پر پائریٹڈ سافٹ ویئر تقسیم کرتی تھی، جس کے نتیجے میں ملٹی نیشنل کارپوریشنز سے قانونی کارروائی کی گئی۔ ایسے جرائم سے نمٹنے کے لیے املاک دانش کے قوانین کو مضبوط بنانا بہت ضروری ہے۔

3۔ سائبر ڈومین میں مالی فراڈ: سائبر فراڈ کے سب سے اہم واقعات میں سے ایک دھوکہ دہی پر مبنی سرمایہ کاری کی اسکیمیں شامل ہے جس میں زیادہ منافع کا وعدہ کیا گیا تھا۔ سائبر جرائم پیشہ افراد نے سرمایہ کاروں کو راغب کرنے کے لیے جعلی ویب سائٹس اور سوشل میڈیا کا استعمال کیا، بالآخر ان کے پیسے سے غائب ہو گئے۔ اس طرح کے واقعات مالی بیداری اور محفوظ آن لائن لین دین کی اہمیت کو اجاگر کرتے ہیں۔

نتیجہ

ڈیٹاپرائیویسی اور سائبر سیکیوریٹی ڈیجیٹل دنیا کے دو ستون ہیں۔ اگرچہ رازداری کے خدشات صارف کے ڈیٹا کی اخلاقی ہینڈلنگ کا مطالبہ کرتے ہیں، سائبر کرائمز کو مضبوط قانونی فریم ورک اور جدید حفاظتی اقدامات کی ضرورت ہوتی ہے۔ تنظیموں، حکومتوں اور افراد کو رازداری کی سخت پالیسیوں کو نافذ کرنے، صارفین کو تعلیم دینے، اور سائبر سیکیورٹی (Cyber security) کے طریقوں کو مسلسل اپ گریڈ کر کے ایک محفوظ ڈیجیٹل ماحولیاتی نظام کی تعمیر کے لیے تعاون کرنا چاہیے۔

کیا آپ مزید کیس اسٹڈیز شامل کرنا یا کسی سیکشن کو بہتر کرنا چاہیں گے؟

7.10 اکتسابی نتائج

- ڈیٹاپرائیویسی کے بنیادی تصورات کو سمجھ سکیں گے۔
- ڈیٹاپرائیویسی کے مختلف حملوں کی شناخت کر سکیں گے۔
- ڈیٹا لنکنگ اور پروفائلنگ کی وضاحت کر سکیں گے۔
- رازداری کی پالیسیوں اور ان کی اہمیت کو سمجھ سکیں گے۔
- مختلف رازداری کی پالیسی زبانوں، جیسے P3P ، XACML اور EPAL ، کو بیان کر سکیں گے۔
- مختلف شعبوں میں ڈیٹاپرائیویسی کے مسائل کا تجزیہ کر سکیں گے۔
- ہندوستان میں سائبر کرائم سے متعلق مختلف کیسز کو سمجھ سکیں گے۔
- ڈیٹا کی رازداری اور سائبر سیکیورٹی کے درمیان تعلق کو سمجھ سکیں گے۔

7.11 کلیدی الفاظ

- ڈیٹاپرائیویسی (Data Privacy)
- رازداری (Confidentiality)
- سالمیت (Integrity)
- دستیابی (Availability)
- فشنگ (Phishing)
- میلویئر (Malware)
- رینسم ویئر (Ransomware)
- مین اِن دی مڈل اٹیک (Man-in-the-Middle Attack)

- اندرونی خطرہ (Insider Threat)
- ڈیٹالنکنگ (Data Linking)
- پروفائلنگ (Profiling)

7.12 نمونہ امتحانی سوالات

معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1۔ ڈیٹاپرائیویسی سے کیامراد ہے؟

2۔ ڈیٹالنکنگ (Data Linking) کیاہے؟

3۔ P3P کی مکمل شکل لکھیں۔

4۔ ڈیٹاپرائیویسی کے کسی ایک حملے کانام لکھیں۔

5۔ GDPR کی مکمل شکل لکھیں۔

مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1۔ ڈیٹاپرائیویسی کے بنیادی تصورات رازداری، سالمیت اور دستیابی کی وضاحت کریں۔

2۔ ڈیٹاپرائیویسی کے مختلف حملوں کی وضاحت کریں۔

3۔ فشنگ، میلویئر اور رینسم ویئر کی وضاحت کریں۔

4۔ ڈیٹالنکنگ اور پروفائلنگ کو مثالوں کے ساتھ بیان کریں۔

5۔ رازداری کی پالیسی کیاہے؟اس کی اہم خصوصیات بیان کریں۔

6۔ P3P، XACML اور EPAL کی وضاحت کریں۔

7۔ مختلف ڈومینز، جیسے طبّی، مالیاتی اور ای کامرس میں ڈیٹاپرائیویسی کی وضاحت کریں۔

8۔ ہندوستان میں سائبر کرائم کی مختلف مثالوں اور چھوٹے کیسز کی وضاحت کریں۔

طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1۔ ڈیٹاپرائیویسی کیاہے؟اس کے بنیادی تصورات، مختلف حملوں، ڈیٹالنکنگ اور پروفائلنگ کو تفصیل سے بیان کریں۔

2۔ رازداری کی پالیسیاں کیاہیں؟رازداری کی پالیسی کی تفصیلات، رازداری کی پالیسی کی زبانیں(P3P، XACML، EPALاور مختلف ڈومینز میں رازداری کی وضاحت کریں۔

3۔ ہندوستان میں سائبر کرائم کی مثالوں اور چھوٹے کیسز پر تفصیلی نوٹ لکھیں۔آن لائن جوئے، دانشورانہ املاک کے جرائم اور مالی فراڈ کو

بھی بیان کریں۔

7.11 تجویز کردہ اکتسابی مواد

1۔ سائبر سیکیورٹی اور ڈیٹا پرائیویسی کی بنیادی کتب

2۔ Data Privacy اور Cybercrime سے متعلق تحقیقی مضامین

3۔ GDPR اور دیگر ڈیٹا پروٹیکشن قوانین

4۔ P3P، XACML اور EPAL سے متعلق مطالعاتی مواد

5۔ ہندوستانی سائبر کرائم سے متعلق کیس اسٹڈیز

6۔ سرکاری سائبر سیکیورٹی اور ڈیٹا پروٹیکشن رپورٹس