پرچہ: ای کامرس
E-Commerce

اکائی: ۲

تحفظ اور خفیہ کاری
Security and Encryption

بی کام
سالِ اوّل

تیار کردہ : افرح فاطمہ، اسسٹنٹ پروفیسر، کمپیوٹر سائنس، مانو
ایڈیٹر : ڈاکٹر محمد سعادت شریف، اسسٹنٹ پروفیسر، شعبہ کامرس، مانو

نظامت فاصلاتی تعلیم
مولانا آزاد نیشنل اُردو یونیورسٹی
حیدرآباد

Unit - II

تحفظ اور خفیہ کاری

Security and Encryption

اس اکائی کے مطالعہ کے بعد آپ واقف ہوں گے:

1. کاروبار میں ذاتی یا شخصی معلومات کی رازداری کے طریقہ سے واقف ہوں گے۔
2. شخصی معلومات کو افشاء سے محفوظ رکھنے کے طریقہ سے واقف ہوں گے۔
3. انٹرنیٹ پر حملوں کے مختلف اقسام سے واقف ہوں گے۔
4. سیکورٹی یا تحفظ کے مختلف اقدامات سے واقف ہوں گے۔
5. Encryption اور اس کے اقسام سے واقف ہوں گے۔
6. Security Channel of Communication سے واقف ہوں گے۔

تمہید

ہر تاجر، صنعت کار یا صارف اپنے معلومات کو خفیہ رکھنا چاہتے ہیں اپنے معلومات کو صرف ضرورت پر ہی فراہم کرتے ہیں۔ ذاتی یا شخصی معلومات کو محفوظ رکھنے کے لئے مختلف تدابیر اختیار کرتے ہیں۔ ٹیکنالوجی کی ترقی نے انٹرنیٹ کی مدد سے معلومات کو افشاء کرنا کافی آسان بنا دیا ہے لیکن سخت تحفظی اقدامات کے سبب معلومات کا افشاء ہونا کافی مشکل ہے۔ عام طور پر سمارٹ فون کو اپنے ذاتی کوڈ نمبر کے ساتھ بند کر دیا جاتا ہے۔ کسی سوٹ کیس کو قفل ڈالنے کے بجائے کسی کوڈ نمبر کے ساتھ بند کر دیا جاتا ہے۔ کوڈ نمبر اپنے ذاتی معلومات کو کسی بھی شخص کی رسائی سے روکتا ہے۔ اپنے مواد کو محفوظ رکھنے کے مختلف تدابیر اختیار کرتے ہیں۔ اس طرح انٹرنیٹ پر فراہم کئے گئے معلومات کو بھی محفوظ رکھنے کے لئے ضروری طریقہ کار اختیار کرتے ہیں۔

تصوراتی پہلو اور اس کی ضرورت(Need and Concept)

ای کامرس کے آپریشن کی کامیابی یا ناکامی کے نتیجے میں متعدد عوامل پروان چڑھتے ہیں۔ صرف اور صرف کاروباری طریقہ کار، ٹیم، گاہکوں، سرمایہ کاروں، مصنوعات، اور اعداد و شمار کی منتقلی اور اسٹوریج کی حفاظت تک ہی یہ محدود نہیں رہتا۔ سائبر سیکورٹی الیکٹرانک تجارت کی سب سے اہم خصوصیات میں سے ایک ہے۔ مناسب پروٹوکول کے بغیر، آن لائن خوردہ فروشوں نے اپنے اور اپنے گاہکوں کو ادائیگی کی دھوکہ دہی کے خطرے میں ڈال دیا۔ سائبر کرائمز سے ناکافی انٹرنیٹ کی حفاظت کی وجہ سے چھوٹے اسٹورز بھی زیادہ سے زیادہ ای کامرس سیکورٹی کے خطرے کا سامنا کرتے ہیں۔ ریکارڈرز یہ ظاہر کرتا ہے کہ پانچ سالہ کاروباری خوردہ فروشوں میں سے ہر ایک کو کریڈٹ کارڈ کے دھوکہ دہی کا سامنا کرنا پڑا ہے۔

ڈیٹا سیکورٹی اور سالمیت کو یقینی بنانے کا سب سے مؤثر ذریعہ خفیہ کاری (encryption) ہے۔ خفیہ کاری ایک عام اصطلاح ہے جس سے مراد ڈیٹا کو انکوڈ کرنے کا عمل ہے، تاکہ تمام طرح کی اطلاعات اور جانکاریوں کو محفوظ طریقے پر انٹرنیٹ کے ذریعہ منتقل کیا جا سکے۔ یہ

بہت ہی آسان طریقے سے غیر متعلقہ افراد کو معلومات فراہم کرنے سے روکتا ہے اور ڈیٹا کی حفاظت کرتا ہے۔ جب کبھی بھی کوئی مواد کی منتقلی کے دوران اسے پڑھنے کی سعی کرتا ہے تو وہ مواد اس کے لئے بے مطلب کا ثابت ہوتا ہے جب تک کے اسے decode نہ کیا جائے۔ خفیہ کاری کا طریقہ کار دوسری جانب یہ ہماری مدد کرتا ہے جیسے کہ صارفین کی پہچان معلوم کرنا، غیر مجازی مواصلات کو اپنے اختیار میں کرنا، مواد کو منتقل کرنا، مواد کی سالمیت کو بحال کرنا، اور اس بات کی یقین دہانی کرانا کہ صارفین اس مواد کی تمام طرح کی ذمہ داریاں لے جس کو اس نے منتقل کیا ہے۔ لہذا خفیہ کاری کا استعمال کیا جاتا ہے یا تو مواصلات کو خفیہ (دفاعی طور پر) رکھنے یا مواصلات میں ملوث لوگوں کی شناخت کرنے کے لئے۔

ای کامرس کے لئے حفاظتی تدابیر (E-Commerce Security Environment)

آن لائن لین دین کے اعداد کا تحفظ کرنا کافی ضروری ہے۔ اعداد یا مواد کی حفاظت کے لئے مختلف تحفظی اقدامات کئے جاتے ہیں تا کہ کسی غیر متعلقہ شخص کو تجارت کے متعلق رسائی ممکن نہ ہو۔ ای کامرس سیکیورٹی، پروٹوکول کا ایک ایسا سیٹ ہے جو ای کامرس ٹرانزیکشنز کی محفوظ طریقے سے رہنمائی کرتا ہے۔ کریڈٹ کارڈ فراڈ ہونے کی صورت میں ہر طرح کے خطرات سے کمپنیوں کی حفاظت کے لئے سخت سے سخت اقدام عمل میں لاتا ہے۔

ای کامرس سیکورٹی میں تین بنیادی تصورات ہیں:

- رازداری
- سالمیت
- دستیابی

رازداری یہ یقینی بناتا ہے کہ صرف اور صرف حقیقی افراد کو ہی معلومات تک رسائی حاصل ہو سکتی ہے۔ غیر حقیقی افراد کو اسکی رسائی نہیں ہو سکتی ہے۔ سالمیت یہ یقینی بناتا ہے کہ کسی بھی آلات پر ذخیرہ کردہ ڈیٹا کو یا مواصلات کے دوران کسی بھی مواد کو ایک غیر حقیقی صارف کبھی بھی تبدیل نہیں کر سکتا ہے۔ دستیابی یہ یقینی بناتا ہے کہ معلومات کا ہر صورت میں دستیاب ہونا ضروری ہے جب بھی اسکی کی ضرورت پڑے۔ سیکورٹی ای کامرس میں اہم کردار ادا کرتا ہے۔ پچھلے چند سالوں سے آن لائن ٹرانزیکشن کی تعداد میں ایک زبردست اضافہ ہوا ہے ساتھ ہی ساتھ خطرے کی تعداد اور ای کامرس سیکورٹی کے خلاف حملوں کی قسم میں بھی برابر کا اضافہ ہوا ہے۔ ایک خطرہ کو اس طور پر بھی بیان کیا جا سکتا ہے "کسی کمزوری کا استعمال کرتے ہوئے غلط طریقے سے غیر مجازی رسائی یا استعمال، معلومات کو افشاں کرنا یا اسکا حصول، معلومات کی چوری یا وسائل کی تباہی، رکاوٹ یا ترمیم"۔ ای کامرس ماحول میں مختلف عوامل شامل ہیں جو ای کامرس نیٹ ورک کی تشکیل کرتے ہیں۔

- دکاندار جو مصنوعات کی خریداری یا خدمات حاصل کرنے کے لئے حکم صادر فرماتا ہے۔
- مرچنٹ جو دکانداروں کو مصنوعات یا خدمات پیش کرتے ہیں
- سافٹ ویئر (ویب سائٹ) جو مرچنٹ سرور یا کسی دوسرے سرور پر انسٹال ہو۔
- حملہ آور جو ای کامرس نیٹ ورک کے لئے خطرناک اور مہلک ثابت ہوتا ہے۔
- ای کامرس نیٹ ورک میں ملوث تمام افراد اور مختلف جماعتیں۔

ای کامرس نیٹ ورک میں محفوظ الیکٹرانک تجارت کو یقینی بنانے کے لئے نیٹ ورک کو محفوظ کرنا ضروری ہے، کلائنٹ (خریدار) کمپیوٹر یا کلائنٹ کی طرف سے ہونے والی ٹرانسمیشن جو مواصلاتی چینل پر گزر رہا ہو، ویب سائٹ سرورر، مرچنٹ سرور یا کسی ہارڈویئر سمیت سبھی طرح کے سرور کے تحفظ کی ضرورت پڑتی ہے۔ یہ صرف واحد ای کامرس سیکورٹی کی تشویش نہیں ہے۔ کلائنٹ کی جانب سے سیکورٹی کی ذمّہ داری صارفین کے لئے اہم سیکورٹی ہے۔ مثال کے طور پر اگر مواصلاتی چینل بلکل ہی secure اور محفوظ ہیں لیکن کلائنٹ کی طرف یا سرور سائڈ کی طرف سے کوئی سیکورٹی کی پیائش نہیں ہے تو معلومات کے افشاء کا خدشہ بنا رہتا ہے۔

ای کامرس میں سلامتی کے خطرات(Security Threats in E-Commerce)

ای کامرس سیکورٹی کا خطرہ کسی بھی طرح کے جانے یا انجانے میں ہونے والی غلطی کی وجہ سے ہو سکتا ہے۔ ای کامرس سیکورٹی کے اندر سب سے زیادہ خطرہ Phishing attack، کریڈٹ کارڈ فراڈ، Hacking، غیر متوقع آن لائن خدمات اور data errors کی وجہ سے ہوتا ہے۔ یہ ایک ایسا حملہ ہوتا ہے جس میں سسٹم اور سافٹ ویئر دونوں کا استعمال ہوتا ہے۔ مشہور تکنیکی حملوں میں سے کچھ ذیل میں بیان کی گئی ہیں:

1. ماہی گیری حملے(Phishing attacks)

ماہی گیری حملوں کا خاص مقصد صارفین کے مواد کو اخذ کرنا ہوتا ہے جیسے کہ login credentials اور کریڈٹ کارڈ نمبر وغیرہ۔ سماجی ویب سائٹ کا استعمال کرتے ہوئے ایک حملہ آور ایک ایسے web page کی ڈیزائننگ کرتا ہے جسکے اندر صارفین اس page کو کھولتے ہوئے اپنے credential data جیسے کہ ای میل id، پاس ورڈ اور دوسرے پیغامات کو input کرتا ہے اور جیسے ہی صارفین submit کے بٹن پر کلک کرتا ہے اس کی ساری کی ساری جانکاریوں سے حملہ آور روبرو ہو جاتا ہے لیکن صارف بے خبر رہتا ہے۔

2. کریڈٹ کارڈ فراڈ(Credit Card Fraud)

ایک ای کامرس سائٹ کے اندر متعدد پہلو اور زاویے ہوتے ہیں جو ایک Hacker کے لئے ادائیگی اور صارف کی معلومات حاصل کرنے کے لئے اندرونی نقطہ کے طور پر کام کرسکتے ہیں۔ Malware کا استعمال کرتے ہوئے ایک حملہ آور کریڈٹ کارڈ کی سبھی معلومات نکالنے کے بعد data کو سیاہ Markets میں فروخت کر دیتا ہے۔

3. DOS حملہ(سروس کی انکار: Denial of Service)

یہ کمپیوٹر سسٹم میں سب سے بڑا خطرہ ہے۔ ابتدائی مراحل میں ایک عام صارف DOS حملہ آور بن سکتا ہے کیونکہ یہ آسانی سے دستیاب ہے۔ سب سے پہلے اسکا استعمال ویب سائٹ کے اوپر مسابقتی پہلو کو دیکھتے ہوئے کیا گیا تھا۔ ایک عرصے تک ان حملوں میں اضافہ ہوا ہے اور کمپیوٹر سسٹمز میں بڑے خطرے سے متعلق عوامل کی وجہ سے یہ زیادہ مہلک اور جدید ترین بن چکا ہے۔ DOS حملے کے اہم مثالوں میں سے TCP SYN، UDP Flooding، اور Ping Flood حملہ، Teardrop حملہ اور Peer-to-Peer حملہ قابل ذکر ہیں۔

4. وائرس کے خطرات(Virus Threats)

کمپیوٹر پر وائرس کا حملہ ایک اہم حملہ ہے۔ اس کو وائرس کے حیاتیاتی شکل سے حاصل کیا گیا تھا کیونکہ اس کے پاس وہ تمام خصوصیات ہیں جیسے چھوٹا ہونا اور مناسب ماحول ملنے پر اسکی تعداد میں اضافہ ہونا۔ عصر حاضر میں سب سے مشہور وائرس حملہ صرف اور صرف کاروباری اعداد و شمار کو تباہ کرسکتے ہیں۔ مثال کے طور پر IROK جو DOS پر مبنی حملہ ہے یہ 10001 بائٹس طویل worm ہے۔

5. ٹروجن ہارسز (Trojan Horses)

اس قسم کا تکنیکی حملہ ایک محفوظ نیٹ ورک کے اندر کمپیوٹر سسٹم کے محفوظ نقطۂ کو کھولنے کے لئے استعمال کیا جاتا ہے۔ یہ ایک ایسی فائل ہوتی ہے جسے صارف دیکھ سکتا ہے یا اسے ڈاؤن لوڈ کرسکتا ہے۔ جیسے ہی صارف اس فائل کو کھولتا ہے ٹروجن کے تباہ کن اثرات سے اپنے آپ کو بچا نہیں پاتا۔ یہ hackers کو محفوظ نیٹ ورک تک رسائی حاصل کرنے میں مدد فراہم کرتا ہے۔

6. غیر تکنیکی حملے(Technical Attacks-Non)

یہ حملہ سب سے آسان ہے اور ان دنوں ہونے والے خطرناک حملوں میں سے ایک ہے۔ بہت سارے کامیاب سیکورٹی حملے جو دنیا بھر کے تنظیم کے لئے خطرہ بن چکا ہے وہ سارے کے سارے غیر تکنیکی حملے ہیں۔

7. سماجی انجینئرنگ (Social Engineering)

بلاشبہ ایک مضبوط سیکیورٹی کی بنیاد رکھی جاسکتی ہے اور اس کو برقرار بھی رکھا جاسکتا ہے، لیکن جب بھی اور جہاں بھی انسانی مداخلت ہو جائے وہاں ایک کمزوری نکھر کر سامنے آتی ہے۔ یہ ایک ایسا آرٹ ہے جو سماجی انجینئرنگ کا استعمال کرتے ہوئے لازمی معلومات حاصل کرتا ہے۔ سوشل انجینئرنگ کے ایک بڑے حصّے میں حملوں کا واقعی پتہ لگانے اور اسے معلوم کرنے کے لئے مشکل امر ہے۔ کیونکہ ہم انسانی عوامل کو پیچیدہ نہیں کرسکتے جیسا ہارڈ ویئر اور سافٹ ویئر میں کیا جاسکتا ہے۔

8. ڈمپسٹر ڈرائیونگ (Dumpster Diving)

یہ ایک ایسا طریقہ ہے جہاں ہیکرز ردی کی ٹوکری (trash) کے ذریعہ غیر قانونی معلومات کو یکجا کرتا ہے اور مفید link تک رسائی حاصل کرلیتا ہے۔ یہ انتہائی کارآمد کاروبار کی معلومات جیسے فون کی فہرست، ہارڈ ویئر ڈسک، Memory اور source کوڈز کے printout کو بھی حاصل کرلیتا ہے۔

9. پاس ورڈ کا اندازہ(Password Guessing)

آج کے اس دور میں حملہ آور اس لائق و قابل ہوتے ہیں کہ صارفین کے پاس ورڈ کا اندازہ لگا سکیں۔ لیکن اس کے لئے صارفین کے معلومات کی ضرورت ہونی بہت ضروری ہے۔ حملہ آور کو صارفین کے بارے میں بہت سے معلومات جیسے اسکی سالگرہ کی تاریخ، عمر، آخری نام، وغیرہ کو جاننے کی ضرورت پڑتی ہے۔ یہ بہت عام ہے کہ اپنا ذاتی معلومات بہت سے صارفین انٹرنیٹ کے اوپر استعمال کرتے ہیں، کیونکہ وہ اسکو مستقبل کے لئے یاد رکھنا چاہتے ہیں۔ لیکن پھر بھی حملہ آور کے نقطہ نظر سے اسکو حاصل کرنے میں بہت زیادہ کوشش کی ضرورت ہوتی ہے جو ایک ایسے سافٹ ویئر کو design کر کے صارفین کے پاس ورڈ کا اندازہ لگا سکیں۔

10. ورک اسٹیشن پر حملہ (Workstation Attack)

سیدھے طور پر اس ورک سٹیشن پر حملہ کر دینا جہاں ویب سائٹ موجود ہے کیونکہ حملہ آور کارکنوں اور ویب سائٹ کی کمزوریوں کو اچھی طرح جانتا اور سمجھتا ہے۔ لہذا، حملہ آور vulnerabilities کے ذریعہ ویب سائٹ کی جڑوں تک رسائی حاصل کرنے میں کامیاب ہو جاتا ہے۔ حملہ آور سب سے پہلے یہ دیکھنے کی کوشش کرتا ہے کہ موجودہ ports کو خودکارانہ طریقے سے یا پہلے سے ہی تیار شدہ ایپلی کیشنز کا استعمال کرتے ہوئے کیسے کھولا جائے۔ اس طرح سے حملہ آور سسٹم تک رسائی حاصل کر لیتا ہے اور ورک سٹیشن کے تمام معلومات کو scan کرتے ہوئے صارفین کے بارے میں تمام معلومات یکجا کر لیتا ہے جیسے کہ id، پاس ورڈ اور دوسری جانکاریاں وغیرہ۔

11. نیٹ ورک سنفنگ (Network Sniffing)

جب ایک خریدار کسی خریداری کی ویب سائٹ پر جاتا ہے اور وہاں ٹرانزیکشن کی جارہی ہو تو sniffing کے ذریعہ حملہ کا امکان بن جاتا ہے۔ جب ایک حملہ آور کسی ایپلیکیشن کا استعمال کر کے sniff کرتا ہے تو کلائنٹ اور سرور کے درمیان تبادلے والے ہونے والے تمام اعداد و شمار یا مواد حاصل کیا جا سکتا ہے۔ نیٹ ورک مواصلات کسی بھی طرح سے انسانی مواصلات کے متبادل نہیں ہے۔ انسانی مواصلات کے اندر ایک تیسرا شخص بھی ہوتا ہے جو بات چیت کو سننے کے بعد آگے منتقل کرتا ہے۔ جبکہ نیٹ ورک مواصلات کی ٹیکنالوجی میں دو جماعتوں کے درمیان اتصال قائم ہوتا ہے اور سارے کے سارے پیغامات data packages میں منقسم ہو جاتے ہیں۔ عام طور پر حملہ آور اپنے آپ کو ممکنہ حد تک خریداروں اور ویب سائٹ کے بیچ رکھنے کی کوشش کرتا ہے تاکہ وہ data packages کو بیچ راستے میں ہی تبدیل کر سکے۔

12. بگ حملہ (Bug Attack)

یہ ایک ایسا حملہ ہے جو خریداروں کی سائٹ یا ویب pages کی سائٹ دونوں پر کیا جا سکتا ہے۔ پہلے سے ہی تیار شدہ آلہ کا استعمال کرتے ہوئے حملہ اس سافٹ ویئر کا پتہ لگا سکتا ہے جو server کو اپنے مقصد کے لئے target کر سکے۔ حملہ آور مزید سافٹ ویئر کے اس patch کا پتہ لگاتا ہے اور bug کو analyze کرتا ہے جو administrators کی جانب سے درست نہیں کیا جا سکے۔

تکنیکی حل (Technological Solutions)

ای کامرس پلیٹ فارم کے اندر الیکٹرانک کامرس کے خطرات کو کم کرنے کے لئے کچھ سیکورٹی خصوصیات کا لازم ہونا نہایت ضروری ہے۔ یہاں کچھ ایسے طریقے ہیں جو آن لائن کاروباری اداروں کو کریڈٹ کارڈ کے پراسیسنگ اور ڈیٹا سیکورٹی کو بہتر بنا سکتے ہیں۔

سیکورٹی کو مضبوط بنانے کے لئے چند اقدامات

1. کثیر پرتوں کے ذریعہ حفاظت (Layered Security-Multi)

اس بات کو یقینی بنانا کہ ای کامرس پلیٹ فارم میں کثیر پرتوں کی سلامتی ہے۔ سائبر کرائم کی سرگرمیوں سے محفوظ اپنے ای کامرس کاروبار کو برقرار رکھنے کا بہترین طریقہ Layered Security-Multi ہے۔ اس بات کو یقینی بنانا کہ (Level Contact Application فارم، search tool اور لاگ ان field) میں security موجود ہے۔

2. تمام ٹرانزیکشنز کی نگرانی (Monitor all transactions)

یقینی بنانا کہ آپ اور آپ کے hosting فراہم کنندہ مشکوک سرگرمیوں کے لئے تمام ٹرانزیکشن کی نگرانی کر رہے ہیں۔ ممکنہ خطرات کی دفاع کے لئے ایک انتباہ کا نظام قائم کرنا جیسے billing address اور shipping address ایک دوسرے کے مماثل نہ ہو یا ایک ہی صارف مختلف قسم کے credit cards کا استعمال کرتے ہوئے بہت سارے orders کر رہا ہو۔

3. باقاعدہ PCI اسکین اور اپ ڈیٹس (Regular PC scan and Updates)

ای کامرس پلیٹ فارم کو مسلسل ممکنہ خطرات سے بچانے کے لئے اکثر تازہ ترین اپ ڈیٹس اور PCI اسکین کا کرنا ضروری ہے ورنہ یہ آن لائن سٹور کو ھدف بنا سکتا ہے۔ خودکارانہ طریقے سے updates کا ہونا، Viruses اور Malware سے ہونے والے خطرات کے امکان کو کم کر دیتا ہے۔

4. ایڈریس کی توثیق (Address Verification System)

محفوظ کریڈٹ کارڈ پروسیسنگ کو مضبوط کرنے کے لئے ایڈریس کی توثیق کا نظام استعمال کرنا چاہیئے جو billing ایڈریس کا موازنہ کرے کہ ایک کسٹمر کے کریڈٹ کارڈ کے اجراء کنندہ فائل پر کیا مذکور ہے۔ ایک AVS خودکارانہ طریقے سے جعلی کوششوں کو قانونی لین دین سے الگ تھلگ کرے گا۔

5. CVV کی ضرورت (Require a CVV)

کریڈٹ کارڈ کے پیچھے Card Verification Value تین یا چار عددی کوڈ میں لکھا ہوتا ہے۔ PCI کے معیار کے تحت خوردہ فروشوں کو اس نمبر کو محفوظ کرنے کی اجازت نہیں ہے، یہاں تک کہ اگر وہ مستقبل کے ٹرانزیکشن کے لئے گاہک کے نام، پتے اور کریڈٹ کارڈ نمبر ریکارڈ کر سکتے ہیں۔ اس کے علاوہ بہت سے Cybercriminals کے پاس کریڈٹ کارڈ نمبر تو ہوتا ہے لیکن ظاہری طور پر کارڈ نہیں ہوتا ہے۔ CVV کی ضرورت دھوکہ دہی سے بچنے کے لئے عمل درآمد کے حالات کو زیادہ سے زیادہ مشکل بنا دیتا ہے۔

6. مضبوط پاس ورڈ کی ضرورت (Require Stronger Passwords)

حملہ آور (Hackers) الگورتھم کا استعمال کرتے ہیں جو صارفین کے پاس ورڈز کا تخمینہ لگاتا ہے۔ یہ پروگرام چار عدد والے پاس ورڈ کے مجموعے پر عمل کرتا ہے جو فوری طور پر صحیح صحیح حرف، عددی پاس ورڈ کو تلاش کرنے کی صلاحیت رکھتے ہے۔ طویل پاس ورڈ کم سے کم ایک خاص حرف یا بڑے حرف کے ساتھ بنا ہوا زیادہ محفوظ ہوتا ہے۔ مضبوط پاسورڈ کے معیار کو لاگو کرنے پر گاہکوں کے مال کی حفاظت ہوتی ہے۔

7. SSL سرٹیفکیٹ (SSL Certificates)

SSL سرٹیفکیٹ کاروبار کے شناخت کی تصدیق کرتا ہے اور چیک آؤٹ کے دوران ٹرانزٹ میں ڈیٹا کو محفوظ کرتا ہے۔ یہ کمپنی اور صارفین کو Hackers سے بچاتا ہے تاکہ وہ مالی یا اہم معلومات باحفاظت رکھ سکے۔

8. ہوسٹنگ فراہم کنندہ کا انتخاب(Choosing a Hosting Provider)

PCI کے مطابق ہونے کے لئے ای کامرس پلیٹ فارم کو کریڈٹ یا ڈیبٹ کارڈ کے ذریعہ ادائیگی کرنے پر سیکیورٹی کی ضمانت کی تمام پالیسیوں اور طریقہ کار پر سختی سے عمل کرنا چاہیے۔ ان میں سے بعض اقدامات جیسے خفیہ کاری، Anti-Malware سافٹ ویئر، وسیع پیمانے پر نگرانی، خطرے کا تجزیہ شامل ہے۔

9. DoS/DDoS حملوں کی محرومی (Protection against DoS/DDoS)

بہت سارے ویب سائٹس ایسے ہیں جنکی Bandwidth ایسی نہیں ہے جو عام طور پر DoS/DDoS حملوں کے خلاف حفاظت کر سکے۔ تاہم، ای کامرس پلیٹ فارم کو ایسا ہونا چاہئے جو اس طرح کے خطرے کا سامنا کر سکے۔

10. کوکیز کو منظم کرنا(Managing Cookies)

جب کوئی خریدار اپنے ذاتی معلومات کے ذریعہ سے اپنے آپ کو کسی ویب سائٹ پر رجسٹر کرتا ہے تو ایک cookie اس کے کمپیوٹر میں محفوظ ہو جاتا ہے تاکہ آئندہ ضرورت پڑنے پر اسے دوبارہ یہ سارے معلومات درج نہ کرنے پڑیں۔ اور یہ ساری کی ساری جانکاریاں ایک attackers کے لئے سود مند ثابت ہوتی ہیں۔ لہذا کوکیز کو استعمال کرنے سے اپنے آپ کو روکنا بہت ضروری ہے۔

11. ذاتی فائروال(Personal Firewall)

خریدار اپنے کمپیوٹر کی حفاظت اپنے ذاتی فائبروال کا استعمال کرتے ہوئے کر سکتا ہے۔ اس کا مقصد کمپیوٹر کے اندر آنے والے تمام ٹریفک کو کنٹرول کرنا ہے۔ ساتھ ہی ساتھ outgoing traffic پر بھی یہ نظر رکھتا ہے۔ مزید firewall کے اندر ایک intrusion detection سسٹم install ہوتا ہے جو کسی بھی طرح کے مداخلت کو برداشت نہیں کرتا ہے۔ جیسے کہ مواد کو access کرنا، ترمیم کرنا یا کمپیوٹر کو غیر فعال بنا دینا وغیرہ۔ لہذا، ضرورت اس بات کی ہے کہ firewall آپ کے کمپیوٹر میں install ہے یا نہیں اسکو یقینی بنائیں۔

12. Encryption and decryption

دو جماعتوں کے درمیان جب مواصلات قائم ہوتا ہے تو تمام ٹریفک کو encrypt کیا جاتا ہے اور client کے encrypted پیغام کو سرور پر بھیج دیا جاتا ہے۔ خفیہ اطلاعات کو ترمیم کرنا ایک attacker کے لئے بہت ہی مشکل ہوتا ہے اور اس سے confidential data کو حاصل کرنا ناممکن بن جاتا ہے۔ اسے symmetric-key الگورتھم یا asymmetric key الگورتھم کے ذریعہ perform کیا جاتا ہے۔

13. ڈیجیٹل دستخط(Digital Signatures)

دستی دستخط کی طرح یہ ایک ڈیجیٹل دستخط ہوتی ہے جو مواد کی حفاظت کرنے میں اپنی کارکردگی کا مظاہرہ کرتا ہے۔ یہ دستخط دو اہم چیزوں کی تصدیق کرتا ہے، سب سے پہلے یہ چیک کرتا ہے کہ کیا ڈیٹا حقیقی client کی جانب سے آرہا ہے اور دوسرا اس بات کی تصدیق کرتا ہے کہ موصول پیغام راستے میں کہیں بھی نظر ثانی نہیں کیا گیا ہو۔ یہ ای کامرس نظام کا سب سے اہم فائدہ ہے۔

14. ڈیجیٹل سرٹیفکیٹ (Digital Certificates)

ڈیجیٹل دستخط صارفین کے بارے میں معلومات یکجا کرنے والے جعلی ویب سائٹ (اندرونی حملے) کے مسائل کو سنبھال نہیں سکتا ہے۔ لہذا، ڈیجیٹل سرٹیفکیٹ کا استعمال کرتے ہوئے اس سارے مسائل کا حل ممکن ہے۔ صارفین کو اس بات کی یقین دہانی کراتا ہے کہ وہ جو ویب سائٹ کا استعمال کر رہا ہے وہ قانونی (legal) ہے۔ کیونکہ اسکو ایک تیسرے فریق یا دوسرے legal parties کے ذریعہ پر اعتماد بنایا جاتا ہے۔ لیکن ایک ڈیجیٹل سرٹیفکیٹ مستقل طور پر یا لامحدود وقت کے لئے پر اعتماد نہیں ہوتا ہے۔ لہذا ہر ایک صارف کی ذمّہ داری بنتی ہے کہ وہ ڈیجیٹل سرٹیفکیٹ کی validity کو وقت بروقت چیک کرتے رہیں۔

15. سرور فائروال (Firewall Server)

ذاتی فائروال کے برعکس ایک ایسا فائروال بھی ہوتا ہے جسے سرور firewall کے نام سے جانا جاتا ہے۔ سرور firewall ایک اعلی درجے کی پروگرامنگ ہے جس کے اندر demilitarized zone technique کا استعمال کیا جاتا ہے۔

Encryption

Encryption ایک ایسا عمل ہے جس میں عام مواد کو ciphertext میں تبدیل جاتا ہے۔ جب ڈیٹا ciphertext میں تبدیل ہو جاتا ہے تو یہ کسی بھی شخص کو اسے پڑھنے یا سمجھنے میں ناممکن بنا دیتا ہے جب تک کہ وہ اپنی اصل شکل میں نہ آجائے۔

اگر ایک file یا Information جو کمپیوٹر میں ہے اسے encrypt کرنا ہو تو اسے secret code میں تبدیل کرنا ہو گا تا کہ وہ کسی اور کے سمجھ میں نہ آئے یا کوئی دوسرا اسے decode یا decrypt نہ کر لے۔ اگر آپ کچھ بھی Encrypt کرنا چاہتے ہیں تو computer آپ سے password پوچھے گا اس کے بعد کوئی بھی اسے سمجھ نہیں پائے گا جب تک اس کے پاس کھولنے کا پاس ورڈ نہ ہو۔ Encryption ڈیٹا کو جاسوسی نگاہوں سے بچاتا ہے۔ یہ ایک ایسا طریقہ ہے جو ڈیٹا کو encode کرتا ہے جو غیر متعلقہ یا غیر مجاز شخص کو اسے دیکھنے یا تبدیل کرنے سے روکتا ہے۔ ان دنوں ہم اکثر Hackers کے بارے میں سنتے ہیں جو بڑی بڑی کمپنیوں، Banks اور Retailers کا مواد چرا لیتے ہیں جو ڈیٹا بیس کے لئے بہت ہی بڑا خطرہ بن چکا ہے۔ اچھی خبر یہ ہے کہ کئی websites ان دنوں آن لائن لین دین کا ڈیٹا encrypted form میں محفوظ ہوتا ہے۔

Using Encryption Technology in E-Commerce

جیسے جیسے E-Commerce کا استعمال ہماری زندگیوں میں بڑھ رہا ہے صارفین کے مواد کو encrypt کرنا بہت ضروری ہو گیا ہے۔ Inventories اور کمپنیوں کے مالیاتی معلومات کی حفاظت کرنا ضروری ہوتا جا رہا ہے۔

جب آپ کوئی بھی Website کی Membership یا Club یا کسی newsletter کے لئے signup کرتے ہیں تو آپکا Personal Information ذاتی معلومات محفوظ ہو جاتا ہے۔

اگر آپ کسی بھی کمپنی سے چیزیں خریدتے ہیں تو آپ کے لین دین کی تفصیلات اس ویب سائٹ میں محفوظ ہو جاتی ہے تا کہ وہ آپ کے افعال کو ریکارڈ رکھ سکے۔

اگر آپ سوچیں تو آپ کے تمام ذاتی معلومات اس کمپنی کے Purchase history میں موجود ہوگا یہاں تک کہ آپ کے کریڈٹ کارڈ کا انفارمیشن بھی اس میں موجود ہوگا۔ اگر اس ویب سائٹ کا ڈیٹا Encrypted نہ ہو تو کوئی بھی hacker اس ویب سائٹ کی security کو توڑتے (break) ہوئے آپ کے سارے انفارمیشن کو آسانی سے جان جائے گا۔

اس سے بچنے کے لئے کمپنیاں اپنے ہی آرگنائزیشن میں ایسی ٹیم یا لوگ منتخب کرتے ہیں جو کمپنی کے ڈیٹا کو حملوں سے بچانے اور سیکوریٹی کو مضبوط بنانے میں اور نئی ٹیکنالوجی تجویز کرنے میں معاون و مددگار ثابت ہوتے ہیں۔ یہ ایک مسلسل لڑائی ہے جو Hackers اور چوروں کے بیچ جاری ہے جو انہیں چوکنا کرتا ہے جو ایسے لوگوں سے ڈیٹا کو بچانے کے لئے چار قدم آگے کی طرف گامزن ہوتا ہے۔

انکرپشن کے اقسام اور طریقہ عمل (Types and Process of Encryption)

Data Encryption کے عمل میں چند بنیادی مراحل (steps) ہوتے ہیں۔ ڈیٹا کو ایک حسابی ضابطہ (Mathematical Formula) سے گزرنا پڑتا ہے جسے Algorithm کہا جاتا ہے جو اسے Encrypted data میں تبدیل کرتا ہے جسے Cipher Text کہا جاتا ہے۔

یہ Algorithm ایک کنجی (Key) بناتا ہے اس کے بعد اس پیغام (Message) کو Key کے ذریعہ encapsulate کیا جاتا ہے۔ Encryption دو قسم کے ہوتے ہیں:

1. Asymmetric Encryption
2. Symmetric Encryption

Asymmetric Encryption

اسے Public Key بھی کہا جاتا ہے جس میں دو mathematically قریبی Keys کا استعمال ہوتا ہے۔ ایک Message کو encrypt کرنے کے لئے اور دوسرا message کو decrypt کرنے کے لئے۔ یہ دونوں keys مل کر ایک key pair بناتا ہے۔

Asymmetric Encryption دو چیزیں فراہم کرتا ہے ایک data encryption اور دوسرا communicating parties کے درمیان validation۔ یہ الگورتھم Symmetric Encryption سے زیادہ محفوظ ہوتا ہے مگر یہ computationally اس سے کم تیز ہوتا ہے۔

Public Key Encryption کے عمل میں پانچ اہم مراحل ہوتے ہیں۔

1. Plain Text: یہ Text Message ہے جس پر Algorithm استعمال ہوتا ہے۔
2. Encryption Algorithm: یہ Plain Text پر Mathematical Operation جیسے Substitution اور Transformation کو انجام دیتا ہے۔

3. keys Private& Public: یہ دونوں keys پیغام کو encrypt اور decrypt کرنے کے لئے استعمال ہوتے ہیں۔
4. Cipher Text: جو message کے اوپر encryption کے عمل کو انجام دینے کے بعد حاصل ہوتا ہے۔
5. Decryption Algorithm: یہ Cipher Text سے Plain Text کو تبدیل کرنے کے لیے استعمال ہوتا ہے۔

Symmetric Encryption

اس کو Private key Encryption یا Single key Encryption بھی کہا جاتا ہے جو Secret Key پر منحصر ہوتی ہے۔ یہ دونوں communicating parties کے بیچ بانٹی جاتی ہے۔ اس الگورتھم میں صرف ایک key ہوتا ہے جسے encryption اور decryption دونوں کے لئے استعمال کیا جاتا ہے۔

Sending Party کو کسی بھی پیغام (message) کو encrypt کرنے کے لئے اسے key secret سے cipher text میں تبدیل کرنا پڑتا ہے تب وہ اس cipher text کو ارسال کرتا ہے۔

اسی طرح receiving party بھی وہی secret key کو استعمال کرتے ہوئے decryption الگورتھم کو عمل میں لاتا ہے جس سے وہ cipher text کو دوبارہ plain text میں تبدیل کرلیتا ہے۔

Encryption Key Symmetric کی مثالیں

1. RSA اور RC4 الگورتھم
2. Data Encryption Algorithm (DES)
3. International Data Encryption Algorithm (IDEA)
4. Skip jack encryption technology جسے United states نے تجویز کیا ہے۔

Symmetric Key Algorithm کی خامیاں

اگر Symmetric Key Algorithm کا استعمال کیا جاتا ہے تو دونوں مرسل (sender) اور مرسل الیہ (receiver) کو key secret بہت ہی محفوظ طریقے سے بھیجنا پڑتا ہے۔ اگر کسی کو secret key معلوم ہو جائے تو وہ آسانی سے decryption algorithm کو بھی معلوم کر سکتا ہے اور communication بھی محفوظ نہیں رہتا۔

Encryption key Symmetric پر دو طریقے سے حملہ ہو سکتا ہے۔

1. Brute Force
2. Crypt Analysis

Brute Force Attack

اس حملہ میں کمپیوٹر کے ذریعہ سارے ممکن مواصلات (Possible Communication) معلوم کئے جاتے ہیں جس سے سادہ تحریر (plain text message) کو معلوم کرلیا جاتا ہے۔

Crypt Analysis Attack

یہ ایک ایسا حملہ ہے جس سے الگورتھم کی ساری خصوصیات معلوم کی جاتی ہے جس سے Plain Text یا key کو معلوم کرلیا جاتا ہے۔

مواصلاتی چیانل کے تحفظات (Security Channels of Communication)

Communication کو محفوظ کرنے کے لئے مندرجہ ذیل آلات استعمال کئے جاتے ہیں۔

1. Secure Socket Layer (SSL)
2. Certificate Authorities (CAs)
3. Virtual Private Networks (VPNs)
4. Secure Electronic Transaction (SET)

Secure Socket Layer

یہ ایک ایسی technique encryption ہے جو انٹرنیٹ پر جانے سے پہلے ڈاٹا کو منتشر (Scramble) کرتا ہے جب کبھی بھی customers کے Browser Web سے merchant کے Browser Web تک بھیجا جاتا ہے۔

Secure Electronic Transaction (SET)

SSL ایک ایسا security protocol ہے جسے اصل میں Net Scape نے متعارف کروایا جسے اب سبھی Web Browsers جیسے کہ Microsoft Internet Explorer بھی حمایت کرتا ہے۔ الیکٹرانک کامرس میں B2C کے سبھی transaction میں SSL کا استعمال ہوتا ہے کیونکہ گاہک کو کوئی Additional Software یا Certificate کو download کرنے کی ضرورت نہیں ہوتی ہے۔ جب ایک گاہک Site Commerce-E کے area Checkout میں داخل ہوتا ہے تب SSL استعمال ہوتا ہے اور یہ گاہک کو بتاتا ہے کہ آپ connection secure کے ذریعہ انفارمیشن حاصل کررہے ہیں اور اسکو key علامت (Symbol) کے ذریعہ مطلع کیا جاتا ہے۔

جب Encryption واقع ہوتا ہے تو صارف اپنے web Browser میں Web Address کی Prefix، http:// کو https:// میں تبدیل کیا ہوا دیکھ سکتا ہے اور Browser Window کے نچلے حصّے میں Padlock دکھائی دینے لگتا ہے۔ دو اہم خصوصیات جو یہ فراہم کرتا ہے وہ security اور confidentiality ہوتی ہے –

SSL گاہک (customer) اور سوداگر (merchant) کے درمیان ایک رابطہ فراہم کرتا ہے۔ جب بھی مرسل (sender) اور مرسل الیہ (receiver) کے درمیان لین دین ہوتا ہے تو SSL اس کو حفاظت دینے کے لئے Encryption فراہم کرتا ہے۔ HTTP-S کے مقابلے میں SSL زیادہ استعمال ہوتا ہے۔

SSL کے اہم مراحل

1. سب سے پہلے Browser Client محفوظ (secure) کنکشن کے لئے ایک بھیجتا بھیجتا ہے۔
2. اس کے بعد Server ایک Digital Certificate کے ذریعہ جواب دیتا ہے جو authentication کے لئے بھیجا جاتا ہے۔

Client اور Server دونوں Session keys کے لئے رضامند ہوتے ہیں۔ Session Key ہی لین دین کے دوران symmetric key کہلاتا ہے –

Certificate Authorities

ای کامرس کو محفوظ بنانے کے لئے بہت سارے کنجیوں (Public keys) کا استعمال کرنا پڑتا ہے اس کے لئے کئی طریقہ کار (Procedures) اور protocols کی ضرورت ہوتی ہے۔ ایک کنجی کو بہت سارے مراحل سے ہو کر کے گزرنا پڑتا ہے جیسے کہ Key Generation، Key Dissemination، Key Revocation وغیرہ ساتھ ہی ساتھ key تبدیل ہونے کے دوران Time Stamping اور Archiving کی بھی ضرورت پڑتی ہے۔

ایک کامیاب Certificate Authority کو قائم کرنے کے لئے اعتماد قائم کرنا ایک بہت ہی پیچیدہ عمل ہے۔ Cryptography کے ماحول میں Certificate Authority ایک ایسا عمل ہے جو Degital Certificate فراہم کرتی ہے۔

Digital Certificate دراصل ایک Digital file ہے جو ایک entity کی Public key کو دوسرے attributes سے باندھ کر رکھتا ہے جو اسکی Identity کو بیان کرتا ہے۔

یہ Entity کوئی بھی ہو سکتی ہے جیسے Person، Organization ایک Website یا Software Application وغیرہ۔

Digital Certificate یہ بیان کرتا ہے کہ ایک Public Key اسی Entity کی ہی ہے۔

Virtual Private Networks

VPN ایک Private Wide Area network ہوتا ہے جو پبلک نیٹ ورک پر چلتا ہے اور Private Network سے کافی سستا ہوتا ہے۔

VPN کو چلانے کے لئے جو تکنیک استعمال ہوتی ہے اسے tunneling کہتے ہیں جس میں Packet Header اور Content دونوں کو Internet protocol (IPsec) کے ذریعہ encrypt کیا جاتا ہے۔

VPN کئی Global Organization کو کاروبار کرنے کے لئے حفاظت فراہم کرتا ہے یہ Expensive Proprietary System کے بجائے Public Internet کو استعمال کرتا ہے۔

Security Measures to Protect Servers

سرور کے اندر سیکورٹی پیدا کرنے کے لئے بہت سارے اقدامات کرنے پڑتے ہیں جن میں سے چند مندرجہ ذیل ہیں:

1. SSH Keys
2. Firewall
3. VPNs and Private Networking
4. Public Key Infrastructure & SSL TLS Encryption
5. File Auditing & Intrusion Detection System
6. Isolated Execution Environment

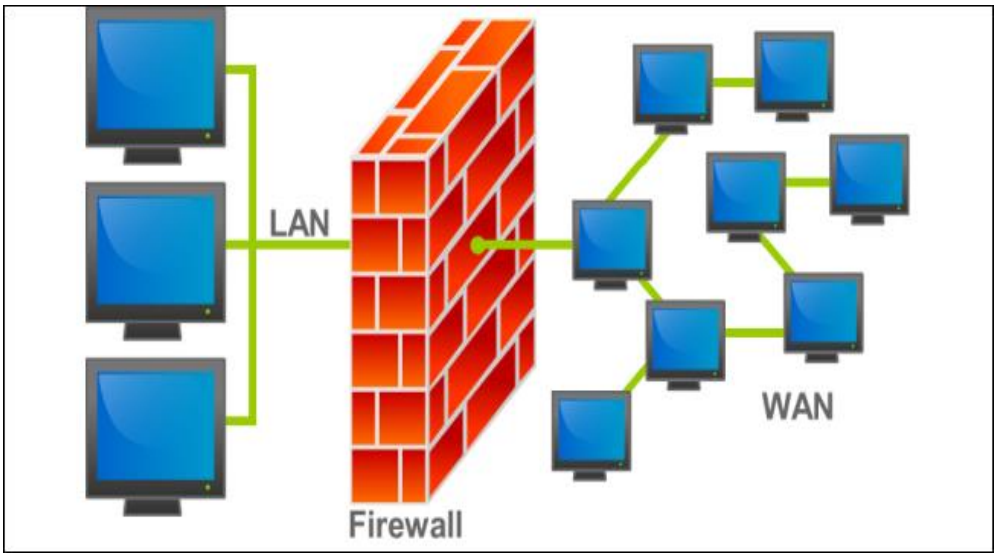
SSH Keys

SSH key دراصل ایک Cryptographic Key ہوتا جو SSH Server کو تصدیق (Authenticate) کرنے کے لئے استعمال ہوتا ہے۔ SSH Key کو Password-based logins کے بغیر بھی استعمال کیا جاسکتا ہے۔ Authentication سے پہلے Private اور Public Key کا Pair بنایا جاتا ہے۔ صارف Private Key کو حفاظت سے رکھتا ہے جبکہ عوامی کنجی (Public Key) کسی سے بھی شیئر کیا جاسکتا ہے۔ SSH Key Authentication کو Configure کرنے کے لئے User کی Public key کو سرور کے Special Directory سے موازنہ کرنا پڑتا ہے۔ جب User کسی بھی سرور کو جوڑتا ہے تب سرور صداقت نامہ مانگتا ہے تب گاہک (client) کو اس کی خانگی کنجی (Public key) سے (Associate) ملانی پڑتی ہے

SSH Client ایک Private key کو اس طریقہ سے استعمال کرتا ہے جیسے وہ اسکی Ownership بیان کررہا ہو جس کے بعد سرور اس Client کو بغیر کسی Password کے connect کرنے کی اجازت دیتا ہے۔

Firewall

Firewall ایک چھوٹا سا ہارڈویئر یا سافٹ ویئر ہوتا ہے جو ساری خدمات کو کنٹرول کرتا ہے تاکہ وہ Network کو بے نقاب نہ ہونے دے۔ یہ Incoming اور Outgoing Packet کو control اور check کرتا ہے۔ اس کا مطلب ہے کہ یہ ہر Port پر accessing کو منجمد اور پابند کردیتا ہے۔



ایک Server پر default کئی خدمات (Services) چلتی رہتی ہیں– Services کو مندرجہ ذیل زمروں میں تقسیم کیا گیا ہے۔

1. Services Public جسے انٹرنٹ کے ذریعہ کوئی بھی گمنام شخص access کرسکتا ہے۔ اسکی مثال ایک Web Server کی ہے جسے Website کے ذریعہ access کیا جاتا ہے۔
2. Services Private جسے صرف چند Accounts Authorized of Group کچھ علاقوں سے ہی access کرسکتے ہیں۔ اسکی مثال Database Control Panel ہے۔
3. Services Internet جسے صرف سرور کے ذریعہ ہی access کیا جاسکتا ہے۔ ان خدمات (services) سے بیرونی دنیا واقف نہیں ہوسکتی۔

اس کی مثال ایک Database کی ہے جو صرف مقامی رابطہ کو accept کرتا ہے۔

Firewall یہ یقینی بناتا ہے کہ Software کو دیئے گئے اقسام کے حساب سے پابندی (restrict) عائد کرتی ہے۔

عوامی خدمات (Services Public) سب کے لئے کھلا رہتا ہے تاکہ سب اس کو access کرسکے جب کہ Private Services مختلف بنیادوں (Criteria) کے حساب سے access کیا جاتا ہے۔

Security Firewall کو کیسے بڑھایا جاتا ہے۔

Firewall، سرور Configuration کا ایک اہم حصّہ ہے۔

اگر آپکی Services میں چاہے کتنی بھی تحفظات (Security) فراہم کریں پھر بھی ان Services کے اندر Firewall کو لگایا جاتا ہے جو اسے تحفظ کے زائد پرتیں (Extra Layer of Protection) فراہم کرتا ہے۔

اگر سافٹ ویئر کے کچھ بھی خدمات (Services) کھلے ہوئے ہوں تو سرور پر حملہ (Attack) ہونے کا خدشہ زیادہ ہوتا ہے

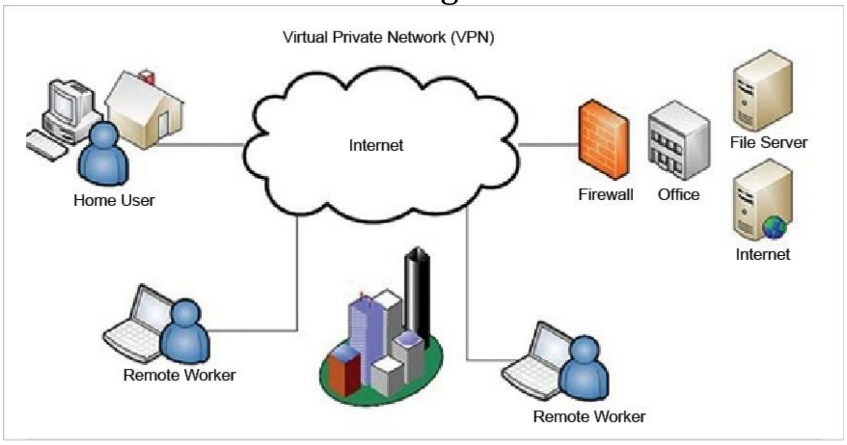
System Linear کے لئے کئی Firewall دستیاب ہیں۔ Firewall کو Setup کرنا بہت اہم ہوتا ہے اور یہ کچھ ہی لمحوں میں Set ہو جاتا ہے۔

VPNs & Private Network

Private Networks ایسے Networks ہوتے ہیں جو صرف کچھ ہی لوگوں کے لئے دستیاب ہوتے ہیں۔

VPN ایک Remote Computer کے درمیان Secure Connections بناتا ہے۔ یہ ایک Private Local Network کی طرح ہوتا ہے جس کی وجہ سے Servers کو Configure کیا جاتا ہے اور Remote Servers کو ایک Secure Connection فراہم کرتا ہے۔

VPN Figure


Virtual Private Network (VPN)
Internet
Home User
Firewall
Office
File Server
Internet
Remote Worker
Remote Worker

خانگی نٹ ورک (Private Network) کے بجائے اگر عوامی یا سرکاری نٹ ورک (Public Network) استعمال کیا جائے تو یہ اندرونی ترسیل (Internal Communication) کے لئے بہتر ہوتا ہے کیونکہ اس Network کو دوسرے Users بھی استعمال کرتے ہیں۔ سب سے بہتر طریقہ ہے کہ تحفظی اقدامات (Security Measures) کا استعمال کیا جائے جو Private Communication فراہم کرتا ہے جو کافی محفوظ ہوتا ہے۔

سوالات

اپنے معلومات کی جانچ کیجئے۔

1. خالی جگہوں کو پر کیجئے۔

1. صارفین کے معلومات کو حاصل کرنے کے لئے ------------------------- حملہ کیا جاتا ہے۔
2. سافٹ ویئر پر حملوں کے چند نام --- ہیں۔
3. آن لائن میں --- ایک اہم عامل ہے۔
4. کاروبار کے شناخت کی تصدیق ----------------------------------- سرٹیفکیٹ کرتا ہے۔
5. DOS کا پھیلاؤ ---ہے۔

2. صحیح غلط کی نشاندہی کیجئے۔

1. Security Multilayered سائبر کرائم کو روکنے کی تکنیک کا نام ہے۔ (_____________)
2. کمپیوٹر پر حملہ وائرس کی وجہ سے ہوتا ہے۔ (_____________)
3. انٹرنیٹ کے بغیر آن لائن لین دین واقع ہوسکتے ہیں۔ (_____________)
4. کریڈٹ کارڈ کے پیچھے ۳ اعداد کا کوڈ ہوتا ہے۔ (_____________)
5. ڈیجیٹل دستخط سے معلومات کو محفوظ رکھنے میں مدد ملتی ہے۔ (_____________)

3. سوالات کے جوابات لکھیں۔

1. ڈیجیٹل سرٹیفکیٹ کسے کہتے ہیں؟
2. سافٹ ویئر پر حملوں کے مختلف اقسام کو بیان کیجئے؟
3. تحفظ (Security) سے کیا مراد ہے؟ وضاحت کیجئے۔
4. ای کامرس کے حفاظتی تدابیر کو بیان کیجئے۔
5. Encryption سے کیا مراد ہے؟ وضاحت کیجئے۔
6. فائر وال کسے کہتے ہیں؟