تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- بیک اپس: کیا، کب اور کیسے
- ریکوٹری
- اہم نکات

بیک اپ اور ریکوٹری

جائزہ

اگر آپ لمبے عرصے تک ایک کمپیوٹر یا موبائل آلہ کو استعمال کرتے ہیں تو کبھی نہ کبھی کچھ غلط ہو سکتا ہے جس کے نتیجے میں آپ اپنی ذاتی فائلز، دستاویزات یا تصاویر سے ہاتھ دھو بیٹھیں گے- مثال کے طور پر ہو سکتا ہے کہ آپ حادثاتی طور پر غلط فائلز ڈیلیٹ کر دیں، آپ کا ہارڈویئر ناکارہ ہو جاتے، آپ کا آلہ گم ہو جاتے یا وہ ‹رینسم ویئر› جیسے میلویئر سے متاثر ہو جائے- ان اوقات کے لیئے بیک اپ ہی آپ کی ڈیجیٹل زندگی کی تعمیر نو کا واحد ذریعہ جاتا ہے- اس نیوز لیٹر میں ہم بیک اپس کے بارے میں بتائیں گے کہ وہ کیا ہوتے ہیں، آپ کو اپنی معلومات کا بیک اپ کیسے لینا چاہیئے اور ایک ایسی حکمت عملی کیسے بنانی چاہیئے جو آپ کے لیئے صحیح ہو-

مہمان ایڈیٹر

کیتھ پامگرین ایک سائبر سکیورٹی کے پیشہ ور ہیں اور آئی ٹی سکیورٹی کی صنعت میں ۳۰ سال کا تجربہ رکھتے ہیں- وہ SANS کے سینئر انسٹرکٹر اور SANS SEC301؛ "انٹروڈکشن ٹو انفارمیشن سکیورٹی" کے مصنّف ہیں- کیتھ ایک کامیاب سکیورٹی کنسلٹنگ چلاتے ہیں اور ٹوئیٹر پر **@kpalmgren** کے ذریعے موجود ہیں-

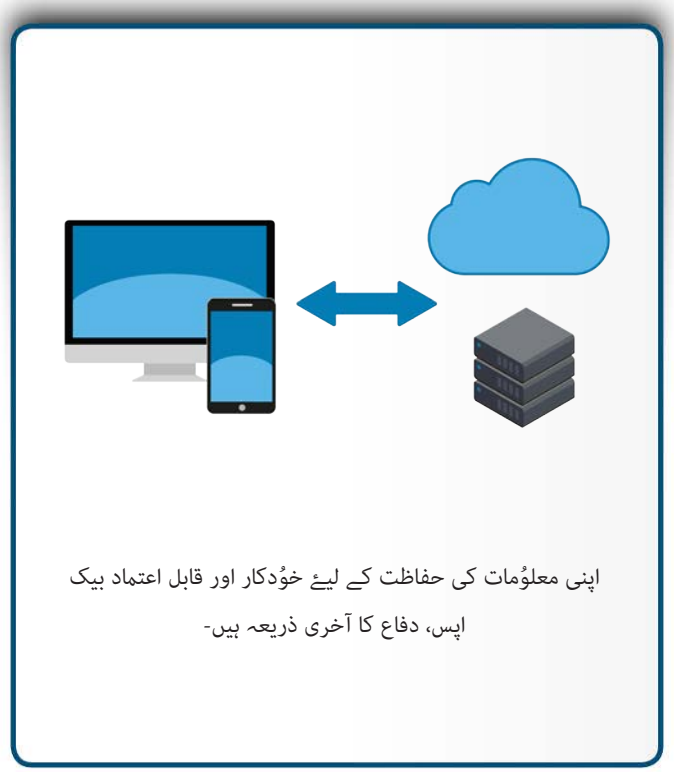
بیک اپس: کیا، کب اور کیسے

بیک اپس آپ کی معلومات کی نقل ہوتے ہیں جنہیں آپ اپنے کمپیوٹر یا موبائل آلات کے علاوہ کسی اور جگہ محفوظ کرتے ہیں- جب آپ کوئی اہم معلومات کھو دیتے ہیں تو آپ بیک اپ کے ذریعے اسے ریکوٹر کر سکتے ہیں- بدقسمتی سے کئی لوگ باقاعدگی سے بیک اپ نہیں لے پاتے ہیں حالانکہ یہ طریقہ کافی آسان اور سستا ہے- سب سے پہلا قدم یہ ہے کہ آپ فیصلہ کر لیں کہ آپ کو کیا بیک اپ کرنا ہے- اس کے دو طریقے ہیں: ۱، وہ اہم معلومات جو آپ کے لیئے اہم ہیں یا ۲، سب کچھ جس میں آپ کا مکمّل آپریٹنگ سسٹم شامل ہے- کئی بیک اپ حل پہلے طریقے کے لیئے پہلے سے کنفیگر ہوتے ہیں اور وہ سب سے زیادہ استعمال ہونے والے فولڈرز کی معلومات کا بیک اپ لیتے ہیں- زیادہ تر آپ کو صرف اس کی ہی ضرورت ہوتی ہے- تاہم اگر آپ کو یہ نہیں پتہ کہ آپ کو بیک اپ کیا کرنا ہے یا آپ زیادہ محتاط ہونا چاہتے ہیں تو آپ مکمّل بیک اپ لیں-

دوسری بات یے کہ آپ کو اس بات کا فیصلہ کرنا ہے کہ آپ کو بیک اپ کتنی کثرت سے لینا ہے- پہلے سے موجود پروگرامز جیسے کہ ایپّل کا ‹ٹائم مشین› یا مائکروسافٹ ونڈوز کا ‹بیک اپ اینڈ ری اسٹور› آپ کو خودکار طور پر بیک اپ اسکیجوُل کرنے کی سہولت فراہم کرتا ہے- بیک اپ کے عام اختیارات میں گھنٹے، روزانہ، ہفتہ وار وغیرہ شامل ہے- دوسرے حل ‹مسلسل حفاظت› فراہم کرتے ہیں جس میں دستاویز کو ہر دفع محفوظ کرتے وقت کسی بھی نئی یا تبدیل ہوئی فائلز کا بیک اپ فورا ہو جاتا ہے - ہمارا مشورہ ہے کہ آپ کم از کم خودکار روزانہ بیک اپس کا استعمال کریں-

آخر میں یہ کہ آپ کو اس بات کا فیصلہ کرنا ہے کہ آپ کو بیک اپ کس طرح کرنا ہے- اپنی معلومات کو بیک اپ کرنے کے دو طریقے ہیں: فزیکل میڈیا یا کلاؤڈ پر منحصر اسٹوریج- دونوں طریقوں کے اپنے فائدے اور نقصانات ہیں- اگر آپ کو نہیں پتہ کہ آپ کو کس طریقے کو استعمال کرنا ہے تو آپ دونوں طریقوں کو ایک ساتھ استعمال کر سکتے ہیں- فزیکل میڈیا وہ آلات ہوتے ہیں جنہیں آپ کنٹرول کر سکتے ہیں جیسے کہ ایکسٹرنل یو ایس بی ڈرائیوز یا وائی فائی تک رسائی والے نیٹ ورک آلات- اپنے فزیکل میڈیا کو استعمال کرنے کا فائدہ یہ ہے کہ آپ بہت زیادہ معلومات کو بیک اپ اور ریکوٹر بہت تیزی

بیک اپ اور ریکوٴری



اپنی معلوٴمات کی حفاظت کے لیئے خوٴدکار اور قابل اعتماد بیک اپس، دفاع کا آخری ذریعہ ہیں-

سے کر سکتے ہیں- نقصان یہ ہے کہ اگر آپ رینسم ویئر جیسے میلویئر سے متاثر ہو جاتے ہیں تو ممکن ہے کہ آپ کا بیک اپ بھی اس سے متاثر ہو جائے- کسی ناگہانی صورت حال میں، جیسے کہ آگ کا لگنا یا چوری ہونا، میں ہو سکتا ہے کہ آپ نہ صرف اپنے کمپیوٹر سے محروم ہو جائیں بلکہ بیک اپس سے بھی- اگر آپ بیک اپس کے لیئے اکسٹرنل آلات کا استعمال کرتے ہیں تو آپ کو اپنے بیک اپ کی ایک نقل کسی دوسری محفوظ جگہ پر ذخیرہ کرنی چاہیئے- اس بات کی بھی یقین دہانی کر لیں کہ جو بیک اپس آپ دوسری جگہ پر ذخیرہ کر رہے ہیں اس کی عنوان کے ذریعے با قاعدہ نشاندہی کی گئی ہو-

کلاؤڈ پر منحصر حل آن لائن سروسز ہوتی ہیں جو آپ کی فائلز کو انٹرنیٹ پر ذخیرہ کرتی ہیں- عموماً آپ ایک ایپلیکیشن کو اپنے کمپیوٹر میں انسٹال کرتے ہیں- پھر یہ ایپلیکیشن آپ کی فائلز کا بیک اپ لیتی ہے آیا کسی شیڈول کے ذریعے یا پھر آپ کے ان فائلز میں ترمیم کرنے کے ساتھ- کلاؤڈ حل کا ایک فائدہ ان کی سادگی ہے- ان میں بیک اپس اکثر خودکار ہوتے ہیں اور آپ ان فائلز تک رسائی کہیں سے بھی حاصل کر سکتے ہیں- چونکہ آپ کی معلومات کلاؤڈ پر موجود ہوتی ہیں اس لیئے گھر میں کسی حادثے کی صورت میں، جیسے کہ آگ لگنے یا چوری ہونے کی صورت میں آپ کے بیک اپ پر کوئی اثر نہیں پڑے گا- کلاؤڈ پر موجود بیک اپس آپ کو میلویئر انفیکشن جیسے کہ رینسمویئر سے متاثر ہونے کی صورت میں آپ کو ریکوٴر کرنے میں مدد فراہم کرتے ہیں کیونکہ کئی کلاؤڈ حل آپ کو میلویئر سے متاثر ہونے سے پہلے والے ورژن پر ریکوٴر کرنے کی سہولت فراہم کرتے ہیں- نقصان یہ ہے کہ اگر معلومات کافی زیادہ ہیں تو ان کا بیک اپ لینے اور ریکوٴر کرنے میں کافی وقت لگ جاتا ہے- پرائیویسی اور سکیورٹی بھی بہت اہمیت کی حامل ہیں- کیا آپ کی بیک اپ سروس مضبوط سکیورٹی کنٹرولز فراہم کرتی ہے جیسے کہ انکرپشن اور ٹواسٹیپ ویریفیکیشن؟

آخری بات یے کہ آپ اپنے موبائل آلات کو نہیں بھولیں- موبائل آلات میں موجود زیادہ تر معلومات جیسے کہ ای میل، کیلنڈر ایونٹس اور کانٹیکٹس پہلے سے ہی کلاؤڈ پر ذخیرہ ہوتے ہیں- تاہم آپ کی موبائل ایپلیکیشن کی کنفگریشن، حالیہ تصاویر اور سسٹم پریفرینسز شاید کلاؤڈ پر ذخیرہ نہ ہوں- آپ اپنے موبائل آلات کے بیک اپ کے ذریعے نہ صرف ان معلومات کو محفوظ کرتے ہیں بلکہ اس طرح آپ کو نئے آلہ میں معلومات منتقل کرنے میں بھی آسانی ہوتی ہے- آئی فون/آئی پیڈ، ایپّل کے آئی کلاؤڈ کے ذریعے خودکار طور پر بیک اپ لیتے ہیں- اینڈرائڈ یا دوسرے موبائل آلات میں اس کا انحصار مینوفیکچرر یا سروس پرووائیڈر پر ہوتا ہے- کچھ صورتوں میں ہو سکتا ہے کہ آپ کو بیک اپ کی مخصوص موبائل ایپلیکیشن خریدنی پڑے-

ریکوٴری

اپنی معلومات کو بیک اپ کرنا صرف آدھا کام ہے؛ آپ کو اس بات کی بھی یقین دہانی کرنی ہے کہ آپ اسے ریکوٴر بھی کر سکتے ہیں- آپ وقفے وقفے سے کسی بھی فائل کو ریکوٴر کر کے دیکھتے رہیں کہ بیک اپس صحیح کام کر رہے ہیں کہ نہیں اور یہ بھی دیکھیں کہ وہ اصل فائل سے مشابہت رکھتے ہیں کہ نہیں- آپ اس بات کو بھی یقینی بنائیں کہ کسی بھی بڑے اپگریڈ (جیسے کسی نئے کمپیوٹر یا موبائل آلہ پر منتقل ہونا) یا کسی بڑی مرمّت سے پہلے (جیسے ہارڈ ویئر تبدیل کرنا) آپ نے مکمّل سسٹم کا بیک اپ لے لیا ہے اور آپ اسے ری اسٹور کر کے بھی دیکھیں-

بیک اپ اور ریکوری

اہم نکات

- اس بات سے قطع نظر کہ آپ کون سے بیک اپ کا حل استعمال کر رہے ہیں، آپ اس بات کو یقینی بنائیں کہ آپ نے بیک اپس کو خودکار بنا دیا ہے اور آپ اسے وقفے وقفے سے دیکھتے رہیں۔
- جب آپ بیک اپ سے کسی سسٹم کو واپس بنا رہے ہوتے ہیں تو اس بات کی یقین دہانی کر لیں کہ اسے استعمال کرنے سے پہلے آپ نے تازہ ترین سکیورٹی کے پیچز اور اپڈیٹس انسٹال کر دی ہیں۔
- آپ پرانے بیک اپس جن کی مزید ضرورت نہ ہو، کو ڈیلیٹ کر دیں تاکہ ان تک کسی غیر اختیار شخص کو رسائی حاصل نہ ہو جاتے۔
- اگر آپ کسی کلاؤڈ کے حل کا استعمال کر رہے ہیں تو آپ ان کی پالیسیز اور شہرت کے بارے میں تحقیق کر لیں اور اس بات کو یقینی بنائیں کہ وہ آپ کی ضروریات پوری کر رہا ہو۔ مثال کے طور پر کیا وہ آپ کی معلومات کو انکرپٹ کرتا ہے؟ کیا وہ مضبوط اوتھنٹیکیشن جیسے کہ ٹواسٹیپ ویریفیکیشن کی حمایت کرتا ہے؟

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں،OUCH! archives تک رسائی حاصل کریں اورSANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سائٹ کا دورہ کریں securingthehuman.sans.org/ouch/archives (انگریزی میں) ۔

اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لئے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'لائک' کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

پاس فریزز:	https://securingthehuman.sans.org/ouch/2017#april2017
ٹُو-اسٹیپ ویریفیکیشن:	https://securingthehuman.sans.org/ouch/2015#september2015
کلاؤڈ سکیورٹی:	https://securingthehuman.sans.org/ouch/2016#november2016
انکرپشن:	https://securingthehuman.sans.org/ouch/2016#june2016
رینسمویئر:	https://securingthehuman.sans.org/ouch/2016#august2016

ایڈیٹوریل بورڈ: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley۔

ترجمہ: شعیب ہاشمی