کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- آپریٹنگ سسٹم کا دائرہ حیات
- اپنے آپ کو محفوظ رکھنا

ونڈوز ایکس پی کا اختتام

جائزہ

ونڈو ز ایکس پی، کمپیوٹر کی تاریخ کا سب سے مقبول ترین آپریٹنگ سسٹم ثابت ہوا ہے۔ ایک ایسا وقت بھی تھا کہ یہ دنیا بھر کے بیشتر کمپیوٹرز میں استعمال ہو رہا تھا۔ تاہم ونڈوز ایکس پی اب پرانہ ہو چکا ہے اور عنقریب مائیکروسافٹ اس کی تمام سپورٹ ختم کر دے گا۔ پہلی دفعہ یہ تقریباً بارہ سال پہلے جاری کیا گیا تھا۔ مائیکروسافٹ نے ونڈزایکس پی کے لئے 8اپریل، 2014تک اینڈ آف لائیف (EOL) ترتیب دیا ہوا ہے۔ اس کا مطلب ہے کہ مائیکروسافٹ اپنے صارفین کےلئے اب کوئی بھی اپڈیٹ یا سیکیورٹی پیچ جاری نہیں کرے گا۔ دنیا کے تقریباً 25فیصد ڈیسک ٹاپ کمپیوٹرز ابھی بھی ونڈوز ایکس پی چلارہے ہیں (صرف ونڈوز 7 اس سے زیادہ مقبول ہے)۔ ایک بار اس کی سپورٹ بند ہو جائے تو یہ لاکھوں لوگوں کیلئے خطرناک ہوگا۔ آپ اس بات کو ذہن میں رکھیں کہ ایکس پی کی وجہ سے صرف گھر کے صارفین ہی اثراندازنہیں ہوں گے کیونکہ یہ ابھی تک بڑے پیمانے پر دفاتر، انڈسٹریل کنٹرول سسٹم، اے ٹی ایم مشین، میڈیکل سسٹم، پوائنٹ آف سیل ٹرمینلز اور دوسری ڈیوائیسز میں استعمال ہو رہا ہے۔ ونڈوز ایکس پی کی سپورٹ ختم ہونے کے بعد جو خطرات لاحق ہوں گے اور ان خطرات سے اپنے آپ کو کیسے بچانا ہے، یہ سب ہم نے نیچے بیان کیا ہے۔

مہمان ایڈیٹر

جیسن فاسن، انکلیو کنسلٹنگ ایل ایل سی میں مائیکرو سافٹ ونڈوز سیکیورٹی پر مہارت رکھتے ہیں۔ وہ سینز کے چھ روزہ کورس "سیکیورنگ ونڈوز وتھ دی کریٹیکل سیکیورٹی کنٹرول (SEC505)" کے مصنف ہیں اور **http://cyber-defense.sans.org/blog/** پر پاور شیل سیکیورٹی اسکرپٹس فراہم کرتے ہیں۔

آپریٹنگ سسٹم کا دائرہ حیات

آپ کو شاید یہ معلوم نہ ہو لیکن آپ کے کمپیوٹر کے آپریٹنگ سسٹم کی زندگی محدود ہوتی ہے۔ جو وینڈر آپریٹنگ سسٹم بناتا ہےوہی آپ کو اس کی اپڈیٹس اور پیچ فراہم کرتا ہے جن کے ذریعے اس میں نئی خصوصیات شامل کی جاتی ہیں، اس کی کارکردگی اور استحکام کو بہتر بنایا جاتا ہے اور آپ کے سسٹم کو محفوظ بنایا جاتا ہے۔ مسئلہ یہ ہے کہ بلآخر ایک وقت ایسا آئے گا جب وینڈر آپ کے آپریٹنگ سسٹم کی مزید سپورٹ فراہم نہیں کرے گا۔کبھی نہ کبھی وینڈر کو اپنے وسائل نئی اور بہترین ٹیکنالوجیز پر مرکوز کرنا ہوں گے۔ اس کا مطلب ہے کہ ایک بار جب آپریٹنگ سسٹم کی سپورٹ ختم ہوجائے تو وینڈر مزید پیچ اور اپڈیٹس فراہم نہیں کرتا یہ جانتے ہوئے کہ آپ کا کمپیوٹر غیر محفوظ ہے اور سائبر مجرمان اسے ہیک کر سکتے ہیں۔ ایسا ہی کچھ ونڈوز ایکس پی کے ساتھ ہونے جا رہا ہے اپریل کے بعد۔ اگرچہ مائیکروسافٹ کو پتہ ہوگا کہ آپ کا ونڈوز ایکس پی کمپیوٹر غیر محفوظ ہے اور سائبر مجرمان فعال طور پر اسکا استحصال کر رہے ہیں، پھر بھی وہ اس کا حل نکالنا چھوڑ دیں گے۔

اپنے آپ کو محفوظ رکھنا

اپنے آپ کو محفوظ رکھنے کیلئے آپ کو ایسا آپریٹنگ سسٹم استعمال کرنا پڑے گا جس کی سپورٹ فعال طور پر موجود ہو۔ اگر آپ متحمل ہو سکتے ہیں تو ہمارا پرزور مشورہ ہے کہ آپ نیا کمپیوٹر خرید لیں۔ بیشتر کمپیوٹرز جن پر ونڈوز ایکس پی چل رہی ہے، آج کل کے نئے آپریٹنگ سسٹمز کو سپورٹ نہیں کرسکتے ہیں۔ اگر آپ نئے کمپیوٹر کے متحمل نہیں ہو سکتے ہیں تو کم از کم آپریٹنگ سسٹم کو اپ گریڈ کرلیں۔ تنظیموں

© The SANS Institute 2014

ونڈوز ایکس پی کا اختتام

کیلئے ونڈوز 8 کے بجائے ونڈوز 7 پر منتقل ہونا قدر کم مشکل ہے کیونکہ ونڈوز7 کا گرافیکل انٹرفیس ونڈوز ایکس پی سے مماثلت رکھتا ہے۔ تاہم ونڈوز8، سافٹ ویئر میں نمایاں بہتری کی وجہ سے پچھلے ورژنز کے مقابلے میں زیادہ محفوظ ہے۔ اس کے علاوہ آپ کچھ دوسرے ونڈرز کے آپریٹنگ سسٹمز پر بھی غور کر سکتے ہیں جیسے کہ Apple کا Mac OS X۔ دونوں صورتوں میں آپ کے پاس آپریٹنگ سسٹم تبدیل کرنے کا وقت ابھی ہے۔ آپ کے پاس انتظار کرنے کا زیادہ وقت نہیں ہے۔ اگر آپ باآسانی پہلے ونڈوز ایکس پی کو تبدیل نہیں کر سکتے ہیں تو مندرجہ ذیل اقدامات پر غور کریں۔

ایک بار ونڈوز ایکس پی کی سپورٹ ختم ہوجائے تو اپنے آپ کو محفوظ رکھنے کا بہترین طریقہ یہ ہے کہ آپ ایسے نئے آپریٹنگ سسٹم پر منتقل ہو جائیں جسے ونڈر فعال طور پر سپورٹ کرتا ہو اور اس بات کی تاکید کرے کہ وہ ہمیشہ موجودہ آپریٹنگ سسٹم ہو۔

- آپ اپنا ونڈوز ایکس پی والا کمپیوٹر صرف اس کام یا ایپلیکیشن کے لئے استعمال کریں جس کا استعمال بہت ضروری ہو۔ مثال کے طور پر آپ یا آپ کی تنظیم کوئی ایسی ایپلیکیشن چلا رہے ہیں جو صرف ونڈوز ایکس پی پر چلتی ہو اور یہی وجہ ہے جس کی وجہ سے آپ اُسے اپ اپ گریڈ نہیں کر رہے ہیں۔ اگر یہی صورتحال ہے تو آپ اُس کمپیوٹر کو کسی اور مقصد کیلئے استعمال نہیں کریں جیسے کہ ای میل یا انٹر نیٹ پر براؤزنگ کیلئے۔

- اگر آپ کو ونڈوز ایکس پی والے کمپیوٹر پر براؤزنگ کرنا ضروری ہے تو آپ انٹرنیٹ ایکسپلورر کا استعمال ختم کر دیں اور کسی دوسرے براؤزر، جیسے کہ موزیلافائیرفاکس، گوگل کروم یا اوپرا، پر منتقل ہوجاائیں۔ اس بات کی ہمیشہ تاکید کرلیں کہ آپ کا براؤزر موجودہ ہے اور اس کا وینڈر ونڈوز ایکس پی پر اس کی حمایت جاری رکھے ہوئے ہے۔

- ایسی تمام ایپلیکیشنز کا استعمال ختم کر دیں جو ونڈوز ایکس پی میں پہلے سے ہی موجود ہوں اور انٹر نیٹ کے ذریعے فائل کھولتی ہوں جیسے کہ ونڈوز میڈیا پلیئر۔ اس کے بجائے آپ دوسرے ونڈرز کی ایسی علیحدہ ایپلیکیشنز کا استعمال کریں جو فعال طور پر اپڈیٹ ہوتی رہیں اور موجودہ ہوں۔

- آپ نیٹ ورک سیکیورٹی کی سروس استعمال کرنے پر غور کریں، جیسے کہ اوپن ڈی این ایس، جو کہ مفت سروس ہے۔ اس طرح کی سروس آپ کے سسٹم کو جانی پہچانی مضر ویب سائیٹس پر جانے سے روکتی ہیں۔ اس کے علاوہ اگر آپ کا کمپیوٹر مشہور باٹ نیٹ کمانڈ اور کنٹرول سرورز سے منسلک ہونے کی کوشش کرتا ہے تو کچھ سروسز اُس کی نشاندہی کر لیتی ہیں جو اس بات کا اشارہ ہے کہ آپ کا سسٹم متاثر ہو چکا ہے۔

- اس بات کو یقینی بنائیں کہ جو سیکیورٹی سافٹ ویئر آپ نے انسٹال کیا ہے، جیسے کہ اینٹی وائرس، اس کی دیکھ بھال اور سپورٹ ونڈوز ایکس پی پر فعال طور پر موجود ہے۔

ونڈوز ایکس پی کا اختتام

- اگر آپ کے کمپیوٹر کو انٹر نیٹ سے منسلک ہونے کی ضرورت نہیں ہے (مثال کے طور پر آپ اسے صرف ورڈ کی پراسیسنگ کے لیئے استعمال کرتے ہیں) تو آپ اسے نیٹ ورک سے منقطع کردیں۔ اگر کمپیوٹر کو نیٹ ورک سے منسلک کرنا ضروری ہے تو آپ اس بات کا یقین کرلیں کہ وہ فائروال کے پیچھے ہو اور ہوسٹ فائروال اس کی جانب آنے والی کسی بھی ٹریفک کو روک رہا ہو۔ تنظیموں کیلئے آپ کو تمام ونڈوز ایکس پی کمپیوٹرز کو ایک علیحدہ نیٹ ورک میں رکھنا پڑے گا تاکہ اگر وہ متاثر ہوں تو بقیہ تنظیم اُس سے متاثر نہ ہو۔

- آپ اپنے ونڈوزایکس پی کمپیوٹرز کا ڈیٹاباقاعدگی سے بیک اپ کرتے رہیں تاکہ اگر کبھی وہ متاثرہوں تو آپ اُس کےلئے تیار رہیں۔ ان میں سے کم از کم ایک بیک اپ کو آپ آف لائن رکھیں جیسے کہ منقطع کی ہوئی یو ایس بی ڈرائیو میں۔ اگر آپ اپنے سسٹم کو بحال کرنے پر مجبور ہوں تو آپ اُسے نئے کمپیوٹر پر بحال کرنے کیلئے ضرور غور کریں۔ اگر آپ اپنے کمپیوٹر کو ونڈوز ایکس پی پر دوبارہ بحال کرتے ہیں تو اس بات کا قوی امکان ہے کہ وہ پھر سے متاثرہو جائیں۔

اگر آپ اپنی تنظیم میں ونڈوز ایکس پی استعمال کر رہے ہیں تو آپ کے آجر کو کچھ اضافی اقدامات اُٹھانا پڑیں گے۔ یاد رکھیں کہ یہ اقدامات صرف مختصر مدت کے لئے کارآمد ہیں۔ یہ آپریٹنگ سسٹم کو اپڈیٹ کرنے یا اُسے صحیح طرح سے محفوظ کرنے کا نعم البدل نہیں ہے۔ آج یا کل آپ کو نئے سسٹم پر منتقل ہونا ہی پڑے گا۔

مزید جائیے:

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں، OUCH! archives تک رسائی حاصل کریں اور SANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سایٹ کا دورہ کریں http://www.securingthehuman.org (انگریزی میں) ۔

اردو ایڈیشن

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

وسائل:

مائیکروسافٹ EOL کے علانات:
www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx
اوپن ڈی این ایس:
www.opendns.org
مائیگریشن میں رہنمائی کے لئے دستاویز:
http://www.zdnet.com/windows-xp-end-of-life-migration-guide-7000023800/
OUCH: بیک اپ اور اس کی بحالی:
http://www.securingthehuman.org/ouch/2013#september2013

OUCH! کی اشاعت SANS Secure The Human Program کے ذریعے ہوتی ہے اور اسے Creative Commons BY-NC-ND 3.0 License کے تحت تقسیم کرنے کی اجازت ہوتی ہے۔ آپ اس نیوز لیٹر کو تقسیم سکتے ہیں اگر آپ اس کا حوالہ دیں ، اس میں کوئی تبدیلی نہ کریں اور نہ ہی اسے تجارتی مقاصد کے لئے استعمال کریں ۔ ترجمے اور مزید معلومات کے لئے ouch@securethehuman.org پر رابطہ کریں

ایڈیٹوریل بورڈ: بل وے مین، والٹ اسکریونز، فل ہوفمن، لینس اسپڑنر، کارمن رولی ہارڈی۔

ترجمہ: شعیب ہاشمی