مئی ۲۰۱۶ OUCH!

کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- چیزوں کا انٹرنیٹ / انٹرنیٹ آف تِھنگز (IoT)
- IoT کو درپیش مسائل
- اپنے IoTآلات کی حفاظت

چیزوں کا انٹرنیٹ / انٹرنیٹ آف تِھنگز (IoT)

انٹرنیٹ آف تِھنگز (IoT) کیا ہے؟

مہمان ایڈیٹر

جیمز لائن (@jameslyne) سکیورٹی کی فرم سافوز میں سکیورٹی ریسرچ کے عالمی سربراہ ہیں- وہ خوُد ساختہ ‹بہت بڑے گیک› ہیں- اُن کی تکنیکی مہارت سکیورٹی کے کئی شعبوں میں ہے- وہ SANS انسٹیٹیوٹ کے سرٹیفائڈ انسٹرکٹر ہیں اور اکثر سکیورٹی کی صنعت سے متعلق کانفرنسز میں کلیدی خطیب کے طور پر شرکت کرتے ہیں-

ماضی میں ٹیکنالوجی نسبتاً آسان ہوتی تھی، آپ صرف اپنے کمپیوٹر کو انٹرنیٹ سے مُنسلک کرتے تھے اور اُسے روز مرّہ کی سرگرمیوں کے لیۓ استعمال کرتے تھے- پھر موبائل آلات جیسے کہ موبائل فُون اور ٹیبلیٹ، کے ہماری زندگیوں میں آنے سے ٹیکنالوجی میں مزید جدت آگئی- اِن آلات نے ایک ڈیسک-ٹاپ کی تمام تر طاقت کو آپ کی جیب میں لا کر رکھ دیا ہے- جہاں اِن آلات کو کہیں بھی لے کر گھُومنا آسان ہو گیا ہے وہاں اِن میں کئی سکیورٹی خدشات بھی لاحق ہو گئے ہیں-

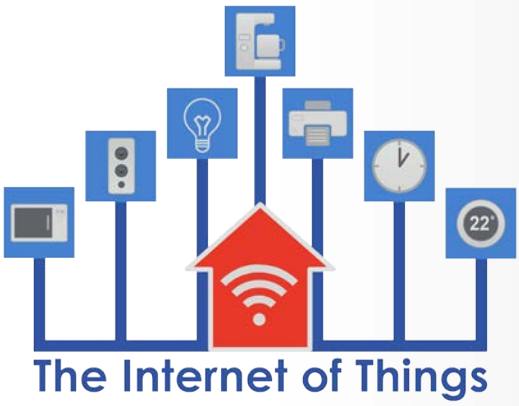
اب اگلی تکنیکی جِدّت انٹرنیٹ آف تِھنگز (چیزوں کا انٹرنیٹ) ہے- انٹرنیٹ آف تِھنگز، جسے مختصراً IoT (آئی او ٹی) بھی کہتے ہیں، کا مقصد روز مرّہ استعمال کے آلات کو انٹرنیٹ سے مُنسلک کرنا ہے- اِن آلات میں دروازے کی گھنٹی سے لے کر لائٹ بلب اور کھلونے کی گُڑیا سے لے کر تھرمواسٹیٹس تک سب شامل ہیں- انٹرنیٹ سے مُنسلک یہ آلات ہماری زندگیاں بہت آسان کر دیتے ہیں- مِثال کے طور پر جب آپ اپنے گھر کی بتّیوں کے قریب جائیں تو وہ خوُدکار طور پر فعّال ہو جاتی ہیں کیونکہ آپ کے فُون کو پتہ چل جاتا ہے کہ آپ اپنے گھر کے پاس پہنچ گئے ہیں- ہر ہفتے ایک نئے آلہ کی آمد کے ساتھ IoT کی مارکٹ بہت تیزی سے آگے بڑھ رہی ہے تاہم موبائل آلات کی طرح IoT آلات کو بھی اُن کے انفرادی سکیورٹی کے مسائل درپیش ہیں- نیوز لیٹر کے اس شُمارے میں ہم آپ کو یہ بات سمجھانے کی کوشش کریں گے کہ IoT آلات کے ساتھ کیا خطرات لاحق ہیں اور آپ اُن کی، اپنے گھر کی اور بالآخر اپنے خاندان کی حفاظت کے لیۓ کیا کر سکتے ہیں-

IoT کو درپیش مسائل

IoT کا سب سے طاقتور پہلوُ یہ ہے کہ ان آلات کا استعمال بہت آسان ہوتا ہے- مِثال کے طور پر جب آپ اپنی کافی مشین پلگ کرتے ہیں تو وہ آپ کے گھر کے ‹وائی-فائی› سے مُنسلک ہونے کی اِجازت مانگتی ہے- تاہم ان تمام آسانیوں کی ایک قیمت بھی ہے- IoT آلات کے ساتھ سب سے بڑی مشکل یہ ہے کہ اُنھیں جو تنظیمیں بناتی ہیں اُن کے پاس سکیورٹی کا کوئی تجربہ نہیں ہوتا، اُن کی تمام تر مہارت گھریلو اپلائنسز بنانے میں ہوتی ہے یا شاید وہ ایک ‹اِسٹارٹ-اپ› ہیں جو کہ مصنوُعات کو مُمکنہ طور پر بہت ہی مؤثّر اور تیز ترین طریقے سے بنانے کی کوشش کر رہے ہوتے ہیں جیسے کہ ‹کِک اسٹارٹر›- یہ تنظیمیں اپنی توجّہ منافع پر مرکوُز رکھتی ہیں نہ کہ سائبر سکیورٹی پر- نتیجتاً کئی IoT آلات جو آج کل خریدے جا رہے ہیں، اُن میں یا تو بہت ہی کم یا پھر سِرے سے سکیورٹی موجوُد ہی نہیں ہوتی- مِثال کے طور پر کُچھ آلات کے بہت معروُف پاس ورڈز ہوتے ہیں، شاید وہ آن-لائن بھی موجوُد ہوتے ہیں اور تبدیل نہیں ہو سکتے ہیں- مزید یہ کہ اُن میں سے کئی آلات میں سکیورٹی کنفیگر کرنے کی صلاحیت یا اختیار موجوُد نہیں ہوتا اور آپ موصوُل ہونے والے اِن آلات کے ساتھ پھنس جاتے ہیں- چیزیں مزید

چیزوں کا انٹرنیٹ / انٹرنیٹ آف تِھنگز (IoT)

اُس وقت بِگڑ جاتی ہیں جب اُن میں سے کئی آلات کو ‹اپگریڈ› کرنا مُشکل ہو جاتا ہے یا اُن میں 'اپگریڈ' کی صلاحیت موجوُد ہی نہیں ہوتی ہے- نتیجتاً آپ کے زیرِاستعمال IoT آلات جلد فرسوُدہ ہو جاتے ہیں کیونکہ اُن میں ایسی کمزوریوں کی نشاندہی ہو جاتی ہے جو ٹھیک نہیں ہو سکتی ہیں جس کی وجہ سے وہ ہمیشہ کے لیئے غیر محفوظ ہو جاتے ہیں-



آپ کو معلوم ہونا چاہئے کہ کون سے IoT آلات آپ کے نیٹ ورک سے مُنسلک ہیں- جب بھی مُمکن ہو آپ اُنھیں علیحدہ کر دیں، اُنھیں اپڈیٹ رکھیں اور مضبوُط پاس-فریزز کے ذریعے اُس کی حفاظت کریں-

اپنے IoT آلات کی حفاظت کرنا

آپ کیا کر سکتے ہیں؟ ہم بالکل چاہتے ہیں کہ آپ اپنے IoT آلات کو مؤثّر اور محفوظ طریقے سے استعمال کریں- یہ آلا ت آپ کو ایسی حیرت انگیز خصوُصیات فراہم کر سکتے ہیں جن سے آپ کی زندگی آسان ہو جاتی ہے، آپ پیسے بچاتے ہیں اور مُمکنہ طور پر اپنے گھر کی سکیورٹی بہتر کر لیتے ہیں- مزید یہ کہ جیسے جیسے ٹیکنالوجی آگے بڑھتی جا رہی ہے آپ کے پاس شاید IoT سکیورٹی آلات خریدنے کے علاوہ کوئی اور چارہ باقی نہ ہو- آپ مُندرجہ ذیل اِقدامات اُٹھا کرIoT آلات اور اپنی حفاظت کر سکتے ہیں-

- **انٹرنیٹ سے صرف ضرورت کے تحت مُنسلک ہوں**: اپنے IoT آلات کو محفوظ بنانے کا سب سے آسان طریقہ یہ ہے کہ آپ اُنہیں انٹرنیٹ سے مُنسلک نہیں کریں- اگر آپ اپنے آلہ کو آن لائن نہیں لے جانا چاہتے تو آپ اُسے وائی-فائی نیٹ ورک سے مُنسلک نہیں کریں-
- **علیحدہ وائی-فائی نیٹ ورک**: اگر آپ کو اپنے IoT آلات کو آن لائن لے جانے کی ضرورت ہے تو آپ اُن کے لیئے ایک علیحدہ وائی-فائی نیٹ ورک بنانے پر غور کریں- کئی وائی-فائی ایکسس پوائنٹس میں مزید نیٹ ورک بنانے کی صلاحیت موجوُد ہوتی ہے جیسے کہ گیسٹ نیٹ ورک- ایک اور اختیار یہ ہے کہ آپ صرف IoT آلات کے لیئے ایک الگ وائی-فائی ایکسس پوائنٹ خرید لیں- اس سے یہ ہوگا کہ آپ کے IoT آلات ایک علیحدہ نیٹ ورک میں آ جائیں گے اور وہ آپ کے پرائمری یا گھر کے نیٹ ورک سے مُنسلک کمپیوٹر یا موبائل آلات پر حملہ یا اُن کو نُقصان پہنچانے کے لیئے استعمال نہیں ہو سکیں گے(جو کہ ابھی بھی سائبر مجرمان کی اصل دلچسپی ہے)-
- **جب بھی مُمکن ہو اپڈیٹ کر لیں**: آپ اپنے ذاتی کمپیوٹر اور موبائل آلات کی طرح IoT آلات کو بھی اپڈیٹ رکھا کریں- اگر آپ کے IoTآلہ میں خوُدکار اپڈیٹ کا اختیار موجوُد ہے تو آپ اُسے فعّال کر دیں-
- **مضبوُط پاس ورڈز**: آپ اپنے IoT آلہ میں موجوُد کسی بھی پاس ورڈ کو ایک ایسے مُنفرد اور مضبوُط پاس فریز سے تبدیل کر دیں جس کا صرف آپ کو علم ہو- کیا آپ تمام پاس-فریزز یاد نہیں رکھ سکتے ہیں؟ آپ پریشان نہ ہوں کیونکہ ہم بھی ایسا نہیں کر سکتے ہیں- اپنے تمام پاس ورڈز کو محفوُظ طریقے سے ذخیرہ کرنے کے لیئے پاس ورڈ مینیجر استعمال کرنے پر غور کریں-
- **پرائیویسی اختیارات**: اگر آپ کا IoT آلہ آپ کو پرائیویسی اختیارات کم کرنے کی اجازت دیتا ہے تو آپ اُس سے شائع ہونے والی معلوُمات کو محدوُد کر دیں- ایک اختیار یہ ہے کہ آپ اُس کی معلومات شائع کرنے والی کسی بھی صلاحیت کو غیر فعّال کر دیں-

چیزوں کا انٹرنیٹ / انٹرنیٹ آف تِھنگز (IoT)

- **آلہ تبدیل کرنے پر غور کریں**: ایک وقت آئے گا کہ آپ اپنے IoT آلہ کو تبدیل کرنے پر غور کریں گے کیونکہ اُس میں بہت سی ایسی معروُف کمزوریاں ہوں گی جو صحیح نہیں ہو سکتی ہوں یا کُچھ ایسے نئے آلات آگئے ہوں جن میں زیادہ بہتر سکیورٹی ہو-

کوئی ایک ایسا معیار نہیں ہے جو ہر آلہ کے لیئے کارآمد ہو اس لیئے بہتر ہے کہ آپ اپنے آلات کو محفوظ بنانے کے لیئے بہترین طریقوں کو تلاش کریں اور اُن سے متعلق کسی بھی اشاعت کا مطالعہ کریں- بد قسمتی سے زیادہ تر IoT آلات بناتے وقت سائبر سکیورٹی پر توجہ نہیں دی گئی تھی اس لیئے کافی سارے مینوفیکچررز سکیورٹی سے متعلق زیادہ معلومات فراہم نہیں کرتے ہیں، لیکن جیسے جیسے سائبر سکیورٹی کا شعور بڑھتا جا رہا ہے ہمیں اُمید ہے کہ ہم زیادہ سے زیادہ IoT وینڈرز کو اپنے آلات میں سکیورٹی فراہم کرتے ہوئے اور اُسے محفوظ بنانے اور اپڈیٹ کرنے سے متعلق معلومات فراہم کرتے ہوئے دیکھیں گے-

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 http://www.securingthehuman.org (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/2015#april2015
پاس ورڈ مینیجرز:	https://securingthehuman.sans.org/ouch/2015#october2015
اپنے نئے ٹیبلٹ کو محفوظ بنانا:	https://securingthehuman.sans.org/ouch/2016#january2016
اپنے گھر کے نیٹ ورک کو محفوظ بنانا:	https://securingthehuman.sans.org/ouch/2016#february2016

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

ترجمہ: شعیب ہاشمی