LOCKHEED MARTIN

قابل‌دفاع فن تعمیرات

انٹیلی‌جنس پر مبنی دفاع کے لیے ڈیزائن کرکے سائبر سیکیورٹی حاصل کرنا®

سکاٹ‌سی فچ، مائیکل مکن
لاک‌ہیڈ مارٹن کارپوریشن

خلاصہ

حفاظتی‌فن تعمیر کے لیے روایتی نقطہ نظر حملے کے خلاف نظام کو سخت کرنے پر مرکوز ہے۔ واضح توقع یہ‌ہے کہ، ایک بار تعیناتی کے بعد، اس کے خلاف ہونے والے تمام حملوں کو روکنا سسٹم کی ذمہ داری ہے۔ تاہم،وہ نظام جو سختی پر سختی سے انحصار کرتے ہیں وہ حملہ آور کی تکنیکوں، صلاحیتوں اور مقاصد میں‌تبدیلیوں سے سیکھ نہیں سکتے، یا خود کو ڈھال نہیں سکتے۔ اور نہ ہی وہ اس حقیقت کا ازالہ کر سکتے‌ہیں کہ حملہ آور کبھی کبھار کامیاب ہو جاتے ہیں۔ ایڈوانسڈ پرسسٹنٹ تھریٹ (اے پی ٹی) سمیت جدیدترین مخالفین کی جاری کوششوں کے لیے ایسے نظام کی ضرورت ہوتی ہے جن کا فعال طور پر اتنے ہی‌نفیس انداز میں دفاع کیا جا سکے۔ ایک انٹیلی جنس پر مبنی ماڈل جو مختلف قسم کے انٹیلی جنس ذرائع‌سے حملہ آوروں کی سمجھ پیدا کرتا ہے، بشمول خود سسٹم کے ساتھ ان کا تعامل، محافظوں کو مخالفوں‌کے حملوں میں تبدیلیوں کے مطابق ڈھالنے اور ان کی توقع کرنے کے قابل بناتا ہے۔

قابل‌دفاع آرکیٹیکچرز انٹیلی جنس سے چلنے والے دفاع کو سپورٹ کرنے کے لیے سسٹمز کو واضح طور پر ڈیزائن،نافذ کرنے اور برقرار رکھنے کے ذریعے سسٹم فن تعمیر کے لیے ایک متبادل نقطہ نظر کی وضاحت کرتے ہیں۔®طریقوں. نتیجہ انٹیلی جنس اکٹھا کرنے کے لیے سسٹمز میں زیادہ مرئیت کا ایک نیک چکر ہے، انٹیلی جنس‌کا دفاعی اقدامات میں تیز تر ترجمہ، اور نظام کے حفاظتی کنٹرولز میں ان اقدامات کی زیادہ موثر تعیناتی‌ہے۔ مزید برآں، خطرے کی انٹیلی جنس سے فائدہ اٹھایا جا سکتا ہے جب سسٹمز کی تعمیر کو یقینی بنایاجا سکے کہ ان کے ڈیزائن کو موجودہ اور ابھرتے ہوئے خطرات کے مطابق اچھی طرح سے ڈھال لیا جائے۔ اس تصورکو مجموعی طور پر انٹرپرائز تک بھی بڑھایا گیا ہے، جس میں یہ بتایا گیا ہے کہ کس طرح تنظیمیں انٹیلی‌جنس سے چلنے والے دفاعی فریم ورک کو ذہن میں رکھتے ہوئے اپنے سسٹمز اور انفراسٹرکچر کی منصوبہ بندی‌اور تعیناتی کر سکتی ہیں۔

اس‌نقطہ نظر کو لاگو کرتے ہوئے، تنظیمیں ایسے سسٹم بنا سکتی ہیں جو سائبر حملوں کے لیے لچکدار ہوں، اورایسے سسٹم ڈیزائن بنا سکیں جو حملہ آوروں کی تکنیکوں اور مقاصد میں تبدیلی کے لیے لچکدار ہوں۔ قابل‌دفاع آرکیٹیکچرز ایسے نظاموں کو بنانے کے لیے ایک نقطہ نظر فراہم کرتے ہیں جو حملے کے خلاف دفاع کر سکیں،سمجھوتہ سے بچ سکیں، اور مخالف تبدیلیوں کو اپنا سکیں۔

مطلوبہ‌الفاظ:فن تعمیر، کمپیوٹر نیٹ ورک ڈیفنس، انٹیلی جنس، اے پی ٹی، لچک

1.تعارف

کلاسیکیمعلومات کے تحفظ کے اصول ممکنہ حملے کے خلاف نظام کو سخت کرنے پر توجہ مرکوز کرتے ہیں۔ روایتی طور پر، یہ حفاظتیکنٹرولز کی وضاحت کرکے کیا جاتا ہے جو ان حملوں کا مقابلہ کریں گے جو ڈیزائنر کے مطابق نظام کا سامنا کرے گا۔ واضح طورپر، ایک بار آپریشن میں، سسٹم سے توقع کی جاتی ہے کہ وہ اس کے خلاف میدان میں آنے والے کسی بھی حملے کو روک دے گا۔

یہنقطہ نظر جدید معلوماتی نظام کے دفاع کی حقیقت کی عکاسی نہیں کرتا ہے۔ سسٹم خود کو محفوظ نہیں رکھ سکتے۔اور نہ ہی ان سے سال، مہینوں، یا ہفتوں پہلے ڈیزائن کیے گئے جامد کنٹرولز کی بنیاد پر ہر حملے کو روکنے کی توقعکی جا سکتی ہے۔ نظام وقت کے ساتھ مخالفانہ رویے میں ہونے والی تبدیلیوں کو سیکھنے اور خود کو ڈھال نہیں سکتے۔مختصراً کہا کہ اگر کوئی ذہین انسان حملہ کر رہا ہے تو ذہین انسانوں کو دفاع کی ہدایت کرنی چاہیے۔

یہمقالہ ایک متبادل نقطہ نظر کی وضاحت کرتا ہے جو زیادہ درست طریقے سے اس بات کی عکاسی کرتا ہے کہ نیٹ ورکڈ سسٹمزکا کس طرح دفاع کیا جانا چاہیے۔ قابل دفاع آرکیٹیکچرز کی بنیاد پر، انٹیلی جنس پر مبنی دفاع کو سپورٹ کرنے کے لیےواضح طور پر ڈیزائن کیے گئے نظام®تکنیک مخالفین کے مقاصد اور ان کی حکمت عملیوں، تکنیکوں اور طریقہ کار (TTPs) میںجاری تبدیلیوں کا مقابلہ کرنے کے لیے بہتر طور پر موزوں ہیں۔ اس طرح کے نظام مرئیت، نظم و نسق اور زندہ رہنے کی خصوصیاتکو ظاہر کر کے اپنے دفاع کی بہتر مدد کرتے ہیں۔ وہ تنظیمیں جو ان آرکیٹیکچرز کو لاگو کرتی ہیں وہ اپنے ڈیزائن، ڈیولپمنٹاور آپریشنز کے دوران خطرے کی ذہانت سے فائدہ اٹھاتی ہیں۔

مزیدبرآں، تمام سسٹمز اپنے انٹرپرائز، انٹرفیسنگ سسٹمز، اور پڑوسی سسٹمز کے تناظر میں موجود ہیں۔ سسٹم کے سیاق و سباق کو سمجھنا اس کے ڈیزائن اور دفاع کے لیے اہم ہے۔ ایک انٹرپرائز اپنے پورے دائرہ کار میں خطرے کی انٹیلیجنس جمع کر سکتا ہے، اور اس انٹیلی جنس کا استعمال مخالف مقاصد اور TTPs سے نمٹنے کے لیے مشترکہ سیکیورٹیانفراسٹرکچر کی منصوبہ بندی اور نفاذ کے لیے کر سکتا ہے۔ اس طرح، قابل دفاع آرکیٹیکچرز کو قابل دفاع انٹرپرائزکے تصور تک بڑھایا جاتا ہے۔

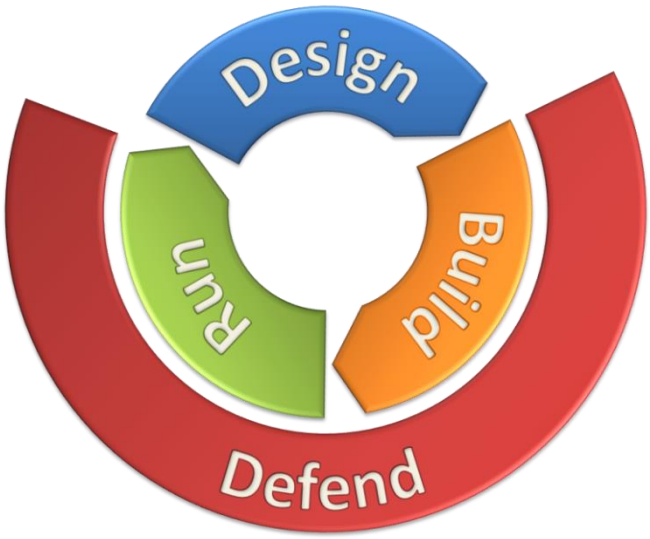
عوامیاور نجی شعبوں میں تنظیموں کے درمیان نیٹ ورک کے حملوں کے خلاف لچک کی اہمیت کی پہچان بڑھ رہی ہے[1] [2] [3] [4]۔ سائبر لچک کی جڑ اس اعتراف میں ہے کہ حملے اور بحالی کے دوران سسٹمز کو اپنی مطلوبہ خدماتفراہم کرنا جاری رکھنا چاہیے۔ اس لحاظ سے، لچک ایک نظام کی حملے، پتہ لگانے، اور بازیابی سے بچنے کی صلاحیتہے۔ لچک ایک حملہ آور کے نقطہ نظر اور مقاصد میں تبدیلیوں کو برداشت کرنے کے لیے نظام کے ڈیزائن کی صلاحیتکی بھی نمائندگی کرتی ہے۔ یا مختلف نقطہ نظر اور مقاصد کے ساتھ نئے حملہ آوروں کا تعارف۔ ڈیفنڈ ایبل آرکیٹیکچراپروچ کو لاگو کرنے والی تنظیمیں ڈیزائن کی موروثی خصوصیت کے طور پر دونوں قسم کی لچک حاصل کرنےکے قابل ہوتی ہیں: سسٹم حملوں کے لیے لچکدار ہوتے ہیں، اور ڈیزائن حملہ آوروں میں ہونے والی تبدیلیوں کے لیے لچکدارہوتے ہیں۔

2نظام کے علم اور خطرے کی ذہانت کا فائدہ اٹھانا

ہچنز،کلوپرٹ، اور امین نے اس ضروری کام کو بیان کیا جو کمپیوٹر نیٹ ورکس کے دفاع میں ذہانت ادا کرتا ہے [5]۔ انٹیلیجنس سے چلنے والے دفاعی عمل میں کلیدی سرگرمیاں، جیسے سائبر کل چین پر مبنی حملوں کا تجزیہ®ماڈل، نئیانٹیلی جنس کی بنیاد پر تاریخی اعداد و شمار کے ذریعے محور، اور بدلتے ہوئے حملوں کے لیے حفاظتی کنٹرول کو ڈھالنےکے لیے، انسانی تعامل اور تجارتی کرافٹ کے کامیاب ہونے کی ضرورت ہے۔

نظاماور کاروباری اداروں کے دفاع میں انسانی ذہانت کے فعال کردار کو تسلیم کرتے ہوئے، تنظیمیں زیادہ موثر سیکیورٹیفراہم کرنے کے قابل ہوتی ہیں۔ ڈیفنڈ ایبل آرکیٹیکچرز پر بنائے گئے سسٹمز نہ صرف محافظوں کے علم اور ذہانتسے فائدہ اٹھاتے ہیں، بلکہ ڈیزائنرز، ڈویلپرز، ٹیسٹرز، اور ایڈمنسٹریٹرز کو بھی جو اس سسٹم کی پوری زندگی میںمدد کرتے ہیں۔ ان کرداروں کی طرف سے نمائندگی کرنے والے مراحل - ڈیزائن، تعمیر، چلائیں، اور دفاع - سبھی اس علمکو نظام میں بانٹنے اور شامل کرنے کے منفرد مواقع پیش کرتے ہیں۔

دوران**ڈیزائن**انجینئرز نظام کے تصور، ضروریات اور ڈیزائنکی وضاحت کرتے ہیں۔ یہ تب ہوتا ہے جب کسینظام کی بہت سی بنیادی حفاظتی خصوصیاتکا تعین کیا جاتا ہے۔ دفاعی آرکیٹیکچرز کوروایتی حفاظتی فن تعمیر سے ممتاز کیا جاتا ہے نہصرف ایک ڈیزائن کرنے کی کوشش پر توجہ مرکوز کرتےہوئے *سخت*سسٹم، لیکن خطرے کی ذہانت اور سسٹمکے خطرے کا تجزیہ استعمال کرکے[1]فن تعمیر کےفیصلوں کی رہنمائی کے لیے، اور انٹیلی جنس سے چلنےوالے دفاعی طریقوں کی ضروریات کو پورا کرنے کےلیے نظام کو ڈیزائن کرنا۔ جیسا کہ اس مقالے میں بعدمیں بیان کیا گیا ہے، ڈیفنڈ ایبل آرکیٹیکچرز پر مبنینظام مرئیت، انتظام اور بقا کی خصوصیات کو ظاہرکرتے ہیں۔ ڈیزائن کے دوران، انجینئرز دستیاب خطرےکی انٹیلی جنس کا بھی تجزیہ کرتے ہیں تاکہ یہتعین کیا جا سکے کہ کون سے حفاظتی کنٹرول سبسے زیادہ موثر ہوں گے۔



شکل1:قابل دفاع آرکیٹیکچرز کا لائف سائیکل

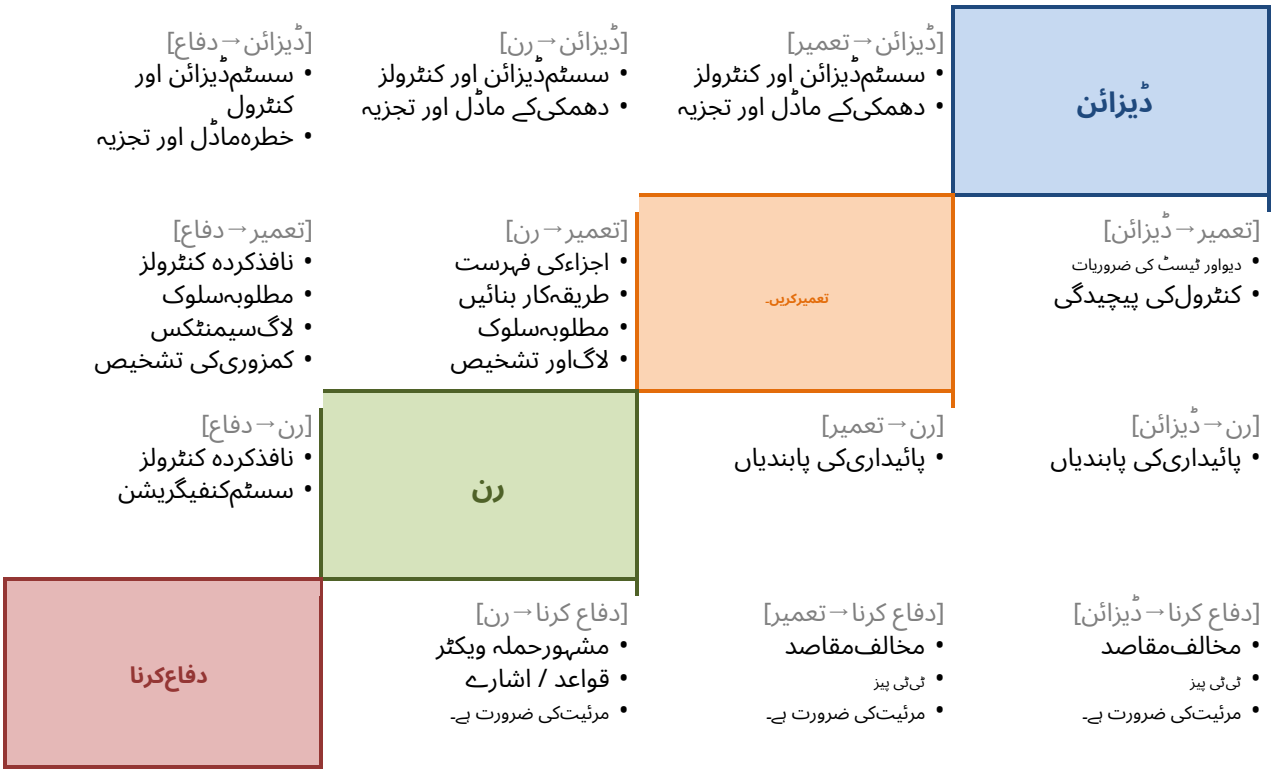
دوران**تعمیر**فیز، انجینئرز کوڈ اور کنفیگریشن کے ذریعے سسٹم کی فعالیت اور سیکیورٹی کنٹرول کو نافذ کرتے ہیں۔ ٹیسٹرزسسٹم کی موروثی حفاظتی خصوصیات (مثلاً، ان پٹ کی توثیق) اور ڈیزائن کے دوران منتخب کیے گئے سیکیورٹیکنٹرولز کی افادیت کی تصدیق کرتے ہیں۔ مختلف قسم کے ٹیسٹ اپروچ استعمال کیے جاتے ہیں، جیسے کنفیگریشنسیٹنگز کا معائنہ، سیکیورٹی کنٹرولز کا مظاہرہ، جامد اور متحرک کمزوری کی جانچ، اور مخالف یا دخول کیجانچ۔ مناسب ٹیسٹ میکانزم کا انتخاب ٹیسٹ کیے جانے والے فنکشنز کے خطرے اور متعلقہ اہمیت سے ہوتا ہے۔

دوران**رن**مرحلہ، منتظمین سسٹم کا انتظام کرتے ہیں اور آخری صارف اسے استعمال کرتے ہیں۔ منتظمین وقت کے ساتھنظام کو برقرار رکھتے ہیں، بشمول آپریشنل ضروریات جیسے پیچنگ اور سسٹم ایڈمنسٹریشن۔ وہ سسٹم کے ڈویلپراور ڈیفنڈر کی تشخیص کو بھی سپورٹ کرتے ہیں، اور محافظوں کے دریافت کردہ نئے اشارے کی بنیاد پر سیکیورٹیکنٹرولز میں تبدیلیاں لاگو کرتے ہیں۔

دوران**دفاع**مرحلہ، انٹیلی جنس تجزیہ کار مخالف سرگرمیوں میں مرئیت کے ذریعے انٹیلی جنس پیدا کرتے ہیں، اور حملوں کاپتہ لگاتے ہیں اور ان کا جواب دیتے ہیں۔ اس میں سسٹم اور اس کے ماخذ کوڈ کی پیداوار، جانچ، اور ترقی کے ماحول کا دفاعشامل ہے۔ محافظ اشارے کو تحفظ اور پتہ لگانے کے قواعد میں ترجمہ کرتے ہیں، اور ان اصولوں کو فعال طور پر نظام کا دفاعکرنے کے لیے تعینات کرتے ہیں۔ وہ ڈیزائنرز، ڈویلپرز، اور منتظمین کو حملے کے ویکٹر میں ہونے والی تبدیلیوں کا بھی جائزہلیتے اور ان سے بات کرتے ہیں۔

ان‌مراحل میں سے ہر ایک، اور وہ کردار جو ان کی حمایت کرتے ہیں، ان کے پاس اشتراک اور شامل کرنے کے لیے اہم علم اور ذہانتہے۔ ان کمیونیکیشنز کا خلاصہ نیچے دیے گئے اعداد و شمار میں کیا گیا ہے، جو قطار کے مرحلے سے کالم کے مرحلے میں معلوماتکی منتقلی کی نشاندہی کرتا ہے۔

[1]اس اخبار میں،*خطرے کی انٹیلی جنس*مخالفین، ان کی مہمات، مقاصد، اور ٹی ٹی پیز کے بارے میں علم سے مراد ہے، جو عام طور پر انٹیلیجنس سے چلنے والے دفاع، انٹیلی جنس شیئرنگ، اور اسی طرح کے طریقوں (مثال کے طور پر، [5]) کے ذریعے جمع ہوتے ہیں۔ *سسٹم کے*خطرات*ناپسندیدہ واقعات یا حالات کا حوالہ دیتے ہیں جو ایک دیئے گئے نظام یا انٹرپرائز کو متاثر کرسکتے ہیں (مثال کے طور پر، [6]). یہ الگلیکن تکمیلی تصورات ہیں، جیسا کہ سیکشن 4.1 میں بیان کیا گیا ہے۔ ان میں فرق کرنے کا ایک ذریعہ، اور زیادہ بوجھ والی اصطلاح "خطرہ" کو واضح کرنے کے لیے ضروری ہے۔

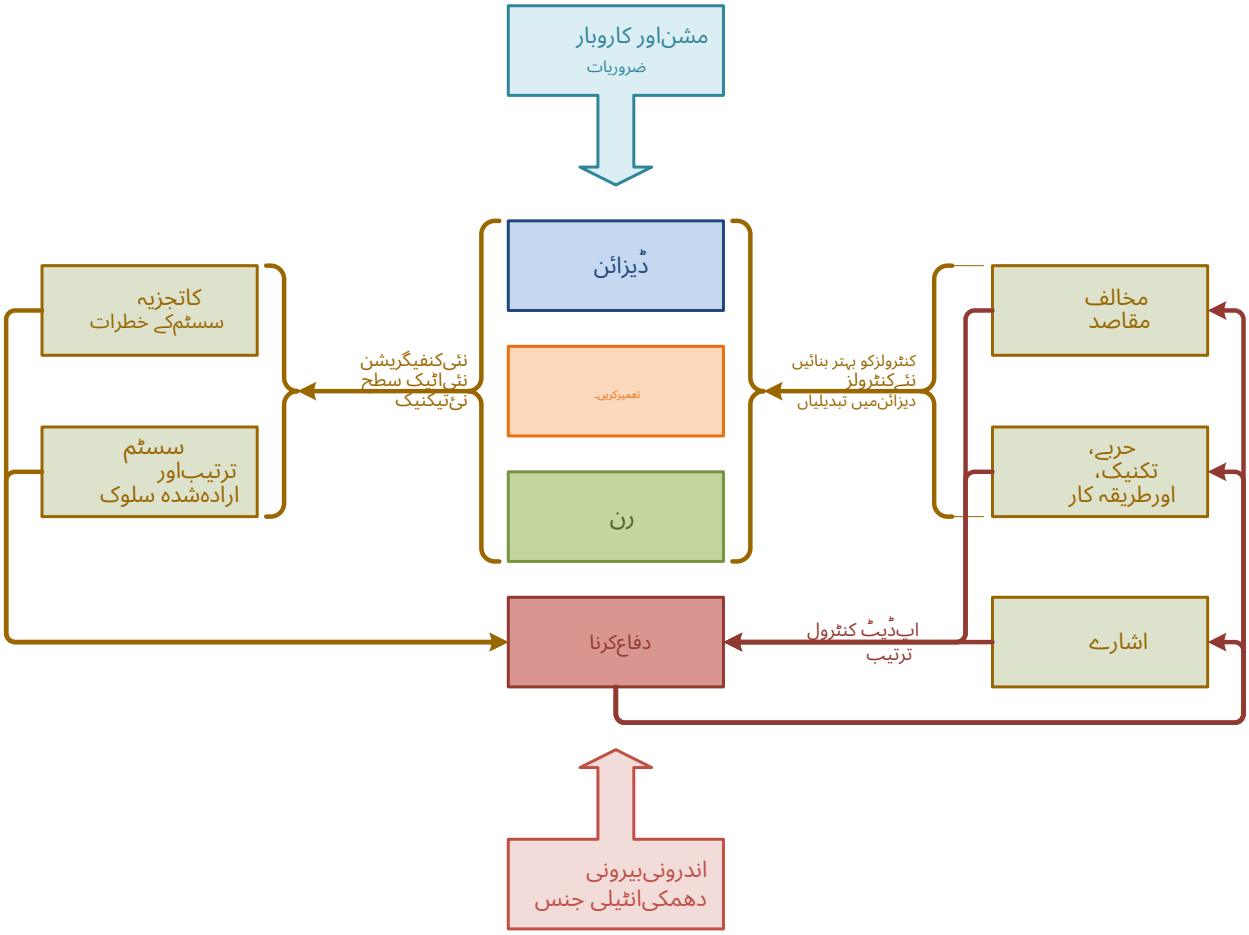


تصویر2:علم کا نمونہ زندگی کے مراحل کے درمیان بہتا ہے۔

اگرچہ‌ان میں سے بہت سے مواصلات کو کلاسیکی سیکیورٹی انجینئرنگ کے طریقوں سے پہچانا جاتا ہے (اور بعض اوقات‌اس پر عمل کیا جاتا ہے)، کئی دفاعی آرکیٹیکچر کے نقطہ نظر سے منفرد ہیں:

- دھمکی‌کے ماڈل اور تجزیہ
- سسٹم‌کی ترتیب اور مطلوبہ سلوک
- مخالف‌سرگرمی کے اشارے
- حکمت‌عملی، تکنیک، اور طریقہ کار (TTPs)
- مخالف‌مقاصد

تصویر3 میں روشنی ڈالی گئی، یہ کمیونیکیشنز ایک تنظیم کو اس قابل بناتی ہیں کہ وہ نظام کے بارے میں معلومات اوراس کے خلاف خطرات کو نظام کے ڈیزائن، تعمیر، چلانے اور دفاع کے طریقے میں مسلسل شامل کر سکے۔



تصویر3:قابل دفاع آرکیٹیکچرز کے چکراتی علم کا بہاؤ

نظام کے خلاف خطرات کا تجزیہ اس وقت پیدا ہوتا ہے جب نظام کو ڈیزائن، تیار اور ترمیم کیا جا رہا ہو۔ یہ تجزیہ اہم اثاثوں کی شناخت کے ساتھ شروع ہوتا ہے، جیسے کہ نظام کے اندر موجود ڈیٹا اور فعالیت۔ سسٹم کے خطرات وہ ناپسندیدہ واقعات یا حالات ہیں جو ان اثاثوں کو متاثر کریں گے [6]۔ جب تک اثاثے موجود ہیں، دھمکیاں بھی۔ مثال کے طور پر، سسٹم کے لین دین کے ڈیٹا کو چوری، چھیڑ چھاڑ، دستیابی میں کمی، یا انکار کا نشانہ بنایا جا سکتا ہے۔ ان خطرات میں سے ہر ایک تنظیم کے مشن اور کاروباری ضروریات پر مختلف ممکنہ اثرات رکھتا ہے۔ ڈیزائنرز اور ڈویلپرز ان خطرات میں سے ہر ایک کو تنظیم پر ان کے اثرات اور ان کو کم کرنے کے لیے دستیاب کنٹرولز کی بنیاد پر متوازن رکھتے ہیں۔ اس تجزیہ کا نتیجہ نظام کے اثاثوں، ان کے خلاف خطرات، اور منتخب کردہ کنٹرولز کی سمجھ ہے۔ اس تجزیہ کے نتائج کو منتظمین اور محافظوں کے ساتھ بانٹنے سے انہیں اہم بصیرت ملتی ہے کہ کون سے اثاثے سسٹم کے لیے سب سے اہم ہیں، اور ان کنٹرولز کا مقصد جو اس کے نتیجے میں منتخب کیے گئے تھے۔

خطرے کے تجزیے کے علاوہ، ڈیزائنرز اور ڈویلپرز سسٹم کی ترتیب اور مطلوبہ رویے کی وضاحت کرتے ہیں۔ اس سے محافظوں کو ایک سسٹم کے ڈیزائن اور اس کے نفاذ کو سمجھنے میں مدد ملتی ہے، جو واقعہ کی آزمائش اور بحالی کے دوران ضروری ہے۔ یہ محافظوں کو متوقع نظام کے رویے کی بنیاد پر ان کا پتہ لگانے کے طریقہ کار کیلیبریٹ کرنے میں بھی مدد کرتا ہے۔ مثال کے طور پر، اگر ایڈمنسٹریٹر تک رسائی کو صرف ایک مخصوص نیٹ ورک پاتھ سے اجازت دینے کے لیے ڈیزائن کیا گیا ہے، تو محافظ جانتے ہیں کہ دوسرے نیٹ ورکس سے انتظامیہ کی کوئی بھی سرگرمی مزید تفتیش کا سبب ہے۔

محافظوں کے پاس ڈیزائنرز، ڈویلپرز اور منتظمین کے ساتھ اشتراک کرنے کے لیے اہم معلومات بھی ہوتی ہیں۔ اکثر عنوان کے تحت اکٹھا کیا جاتا ہے۔*خطرے کی انٹیلی جنس*،ہم نے تین مختلف تجرید کی نشاندہی کی۔ یہ

خطرےکی انٹیلی جنس کی مختلف سطحیں مختلف طریقوں سے سسٹم کے ڈیزائن، نفاذ اور آپریشنز کو متاثر کرتی ہیں۔

سب‌سے بنیادی سطح پر، نئے انکشاف کردہ اشارے ایسے قواعد تیار کرنے کے لیے استعمال کیے جاتے ہیں جو انٹرپرائز کی سطحکے حملے کے تجزیے اور خطرے کی انٹیلی جنس شیئرنگ پر مبنی موجودہ کنٹرولز پر لاگو ہوتے ہیں۔ نئے اشارے عام طور پریہ ظاہر کرتے ہیں کہ مخالف اپنی ٹول کٹس یا انفراسٹرکچر کے حصوں کو تبدیل کر رہا ہے۔ ان تبدیلیوں کا انتظام عام طور پر محافظوںکے ذریعہ کیا جاتا ہے اور مناسب سیکورٹی انفراسٹرکچر منتظمین کے ذریعہ موجودہ سیکورٹی کنٹرولز میں ترتیب اورقواعد میں شامل کیا جاتا ہے۔

تجزیدکی ایک اونچی پرت پر، مخالفوں کے ٹی ٹی پی میں تبدیلیاں نئی قسم کے کنٹرول کو نافذ کرنے کی ضرورت پڑسکتی ہیں‌تاکہ حملے کی نئی اقسام کو حل کیا جاسکے۔ یہ اکثر نئی مخالف مہمات کے وجود کا اشارہ دیتے ہیں یا مخالفین اپنے حملےکرنے کے طریقے میں تبدیلیاں کرتے ہیں، جیسے کہ ای میل سے ویب پر مبنی حملوں میں تبدیلی۔ چونکہ ایک حملہ آور TTPs کو تبدیل کرنے کے لیے لاگت اٹھاتا ہے، اس لیے یہ انفرادی اشارے سے زیادہ پائیدار پتہ لگانے اور تحفظ کے کنٹرول ہوتے ہیں۔اگرچہ TTPs میں کچھ تبدیلیوں کے لیے بنیادی ڈھانچے یا نظام میں ترمیم کی ضرورت ہوتی ہے، لیکن ایک لچکدار بنیادیڈھانچہ محافظوں کو TTPs میں ہونے والی بہت سی تبدیلیوں کے لیے دفاع کو ڈھالنے کی اجازت دیتا ہے۔ TTPs میں مشاہدہشدہ تبدیلیوں کے نتیجے میں آپریشنز اور ڈویلپر کے وسائل کو نئے، زیادہ موثر تخفیف کے لیے دوبارہ مختص کرنے کے لیےکچھ موجودہ کنٹرولز پر زور دیا جا سکتا ہے۔

خطرےکی ذہانت کے تجرید کی آخری تہہ کو مخالفین کے مقاصد کو سمجھنے کے لیے استعمال کیا جاتا ہے۔ اشارے کی دریافتاور ٹی ٹی پی کی کچھ تبدیلیوں کے برعکس، جنہیں زیادہ چستی کے ساتھ حل کیا جا سکتا ہے، مخالف مقاصد میںتبدیلی بنیادی طور پر سسٹم کے ڈیزائن اور کنٹرول کے انتخاب کو متاثر کرتی ہے۔ نظام کی رازداری، سالمیت، اور دستیابیکی ضروریات کے ساتھ مخالفین کے مقاصد کا موازنہ ڈیزائنرز کو نظام کے بارے میں مناسب ڈیزائن کے فیصلےکرنے اور ایسے حفاظتی کنٹرولوں کا انتخاب کرنے کی اجازت دیتا ہے جو نظام کو متوقع خطرات کو مؤثر طریقے سےکم کرتے ہیں۔ مثال کے طور پر، ایک ایسا نظام جس کو دستری بیوٹڈ ڈینیئل آف سروس (DDOS) کے حملے کا سامناکرنا پڑتا ہے اس سے مختلف طریقے سے ڈیزائن کیا جائے گا جس کا مقصد ایسے حملے سے بچنا نہیں ہے۔ یہ ڈویلپرز،ٹیسٹرز، اور منتظمین کو ضروری کنٹرولز کو لاگو کرنے اور برقرار رکھنے اور مناسب ٹیسٹ کے منظرناموں کا انتخابکرنے کی بھی اجازت دیتا ہے۔ موجودہ خطرے کی انٹیلی جنس کے تناظر میں سسٹم کی حفاظتی ضروریات کا تجزیہکرنے سے سسٹم کے خطرے کے انداز کی مزید مکمل تصویر ملتی ہے۔

ان‌تنظیموں کے لیے جنہوں نے دفاعی ڈھانچہ کو ذہن میں رکھتے ہوئے پہلے ہی حفاظتی ڈھانچہ تعینات کر رکھا ہے، محافظ نئے اشارےاور TTPs میں ہونے والی تبدیلیوں کا تیزی سے اور براہ راست جواب دے سکتے ہیں۔ نئی انٹیلی جنس کی بنیاد پر کنٹرول کو ایڈجسٹکرنے کے لیے جتنے کم اقدامات درکار ہوں گے، تنظیم اتنی ہی تیزی سے اپنے مخالفوں کی تبدیلیوں پر رد عمل ظاہر کر سکتی‌ہے۔ اس کی مزید وضاحت سیکشن 5، دی ڈیفنڈ ایبل انٹرپرائز میں کی گئی ہے۔

یہ‌علمی بہاؤ ایک بند-لوپ نیکی کا چکر پیدا کرتا ہے جہاں خطرے کی ذہانت سسٹم کے ڈیزائن اور نفاذ کو متاثر کرتی ہے،جس کے نتیجے میں خود سسٹم کے آپریشنز اور دفاع میں بہتری آتی ہے۔ اس علم کو ان کرداروں میں بانٹنے سے جو ایک‌نظام کو اس کی زندگی بھر میں سپورٹ کرتے ہیں، پوری ٹیم بہتر طریقے سے سسٹم کا دفاع کرنے کے قابل ہوتی ہے۔ نتیجہ‌ایک ایسا نظام ہے جو حملہ کرنے کے لئے لچکدار ہے، اور ایک نظام کا فن تعمیر جو حملہ آوروں کو تبدیل کرنے کے لئےلچکدار ہے۔

3سپورٹنگ انٹیلی جنس پر مبنی دفاع®

اوپربیان کیے گئے علم کے بہاؤ کا فائدہ اٹھاتے ہوئے، تنظیمیں ایسے نظام کو میدان میں لا سکتی ہیں جو ان کے مشن کیضروریات اور مخالفین کی صلاحیتوں اور مقاصد کے مطابق ہوں۔ یہ تنظیموں کو اس بات کی بھی بہتر بصیرت کے ساتھزیادہ مؤثر طریقے سے ان سسٹمز کا دفاع کرنے کی اجازت دیتا ہے کہ نظام کس طرح عام حالات میں کام کرنے کا ارادہرکھتا ہے۔ معلومات کے یہ تبادلے ڈیزائن کے فیصلوں، عمل درآمد کی تجارت، اور نظام کی آپریشنل ضروریات کو آگےبڑھاتے ہیں۔

اس‌معلومات کے تبادلے کے علاوہ، قابل دفاع آرکیٹیکچرز کچھ مشترکہ خصوصیات کی نمائش کرتے ہیں۔ ان خصائص کےساتھ، سسٹمز کو واضح طور پر انٹیلی جنس پر مبنی دفاعی طریقوں کے لیے ڈیزائن کیا گیا ہے، جس سے منتظمین اورمحافظ نظام کے فعال دفاع کو بہتر طریقے سے انجام دے سکتے ہیں۔ ان خصوصیات کا خلاصہ مرئیت، انتظام اور بقاکے طور پر کیا گیا ہے۔

مرئیتانٹیلی جنس سے چلنے والے دفاعی تجزیہ کے لیے ایک اہم اینبلر ہے۔ یہ آپریٹرز اور محافظوں کو نیٹ ورک، آپریٹنگ‌سسٹم اور ایپلیکیشن لیئر پر سرگرمی دیکھنے کی اجازت دیتا ہے۔ یہ مستقبل کی انٹیلی جنس کی بنیاد پر تحقیقات‌کے لیے سرگرمی کا ایک تاریخی ریکارڈ بھی فراہم کرتا ہے۔

انتظامی‌قابلیتاس بات کو یقینی بناتا ہے کہ ایک نظام وقت کے ساتھ برقرار رہ سکتا ہے۔ سسٹم کی حفاظتی کرنسی کو برقرار رکھنے میں‌انتظامی سرگرمیاں شامل ہیں جیسے سسٹم کی پیچنگ اور کنفیگریشن۔ اس میں نئے خطرے کی انٹیلی جنس کی بنیاد پر سسٹم یا اس‌کے ماحول کے سیکیورٹی کنٹرولز کو اپ ڈیٹ کرنے کے قابل ہونا بھی شامل ہے۔ جس رفتار اور درستگی کے ساتھ اپ ڈیٹس کو تعینات کیاجا سکتا ہے اس سے اس بات پر بہت اثر پڑتا ہے کہ اس کا کس حد تک دفاع کیا جا سکتا ہے۔

زندہ‌رہنے کی صلاحیتحملے، سمجھوتہ اور بحالی کے دوران نظام کو اپنی مطلوبہ خدمات فراہم کرنے کی اجازت دیتا ہے۔ جہاں‌کلاسیکی حفاظتی اصول ابتدائی حملے کے خلاف نظام کو سخت کرنے پر توجہ مرکوز کرتے ہیں، وہیں دفاعی آرکیٹیکچرز پس‌منظر کی نقل و حرکت کو برداشت کرنے اور حملے سے بازیابی کو یقینی بنانے کے لیے نظام کی صلاحیت پر بھی توجہ دیتےہیں۔

4قابل دفاع نظام بنانا

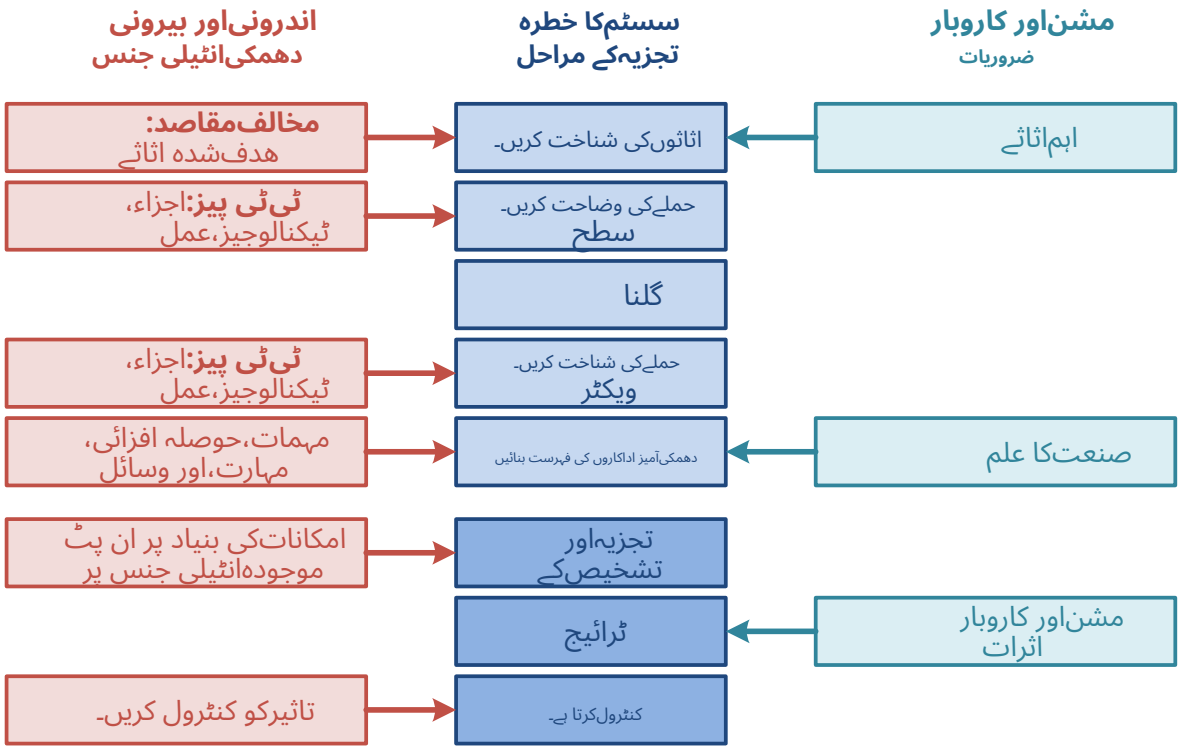
سیکیورٹی‌سسٹم کی موروثی خصوصیت ہے، نہ کہ بعد میں شامل کردہ خصوصیت۔ اسی طرح، قابل دفاع آرکیٹیکچرزپر مبنی نظام مشن کی ضروریات اور خطرے کی ذہانت کو شامل کرتا ہے، اور نظام کے اندرونی حصوں کے طورپر مرئیت، انتظام اور بقا کی خصوصیات کو ظاہر کرتا ہے۔ مندرجہ ذیل حصے بیان کرتے ہیں کہ کس طرح ڈیفنڈ ایبل‌آرکیٹیکچرز کی بنیاد پر سسٹمز کو ڈیزائن، بنانا، چلانا اور ان کا دفاع کرنا ہے۔

4.1قابل دفاع نظام ڈیزائن کرنا

یہ‌ڈیزائنر کی ذمہ داری ہے کہ وہ سسٹم کے ڈیزائن میں قابل دفاع فن تعمیر کی خصوصیات کو تیار کرے۔ جب کہ سیکیورٹی‌ڈیزائن کے لیے روایتی نقطہ نظر کنٹرولز کے انتخاب پر توجہ مرکوز کرتا ہے، ڈیزائنرز کو سسٹم کے اندر موجود اثاثوں،ان کے خلاف خطرات، اور تنظیم کے مشن اور کاروباری ضروریات پر ان خطرات کے اثرات کی سمجھ سے آغاز کرناچاہیے۔ سسٹم کا بنیادی حفاظتی مقصد اس کے اثاثوں کی حفاظت کرنا ہے۔ لہذا ان اثاثوں کے خلاف خطرات ڈیزائن‌کا بنیادی خیال ہیں۔ کمزوریوں اور ڈیزائن کی خامیوں کے برعکس، سسٹم کے خطرات نظام کے لیے حفاظتی مقاصدکے نسبتاً مستحکم سیٹ کی نمائندگی کرتے ہیں۔ جیسا کہ اوپر کہا گیا ہے، جب تک اثاثہ موجود ہے، اسی طرح دھمکیاں‌بھی۔ یہ نظام کے ڈیزائن میں شامل کرنے کے لیے کنٹرولز کی تشخیص اور انتخاب کی بنیاد فراہم کرتا ہے۔

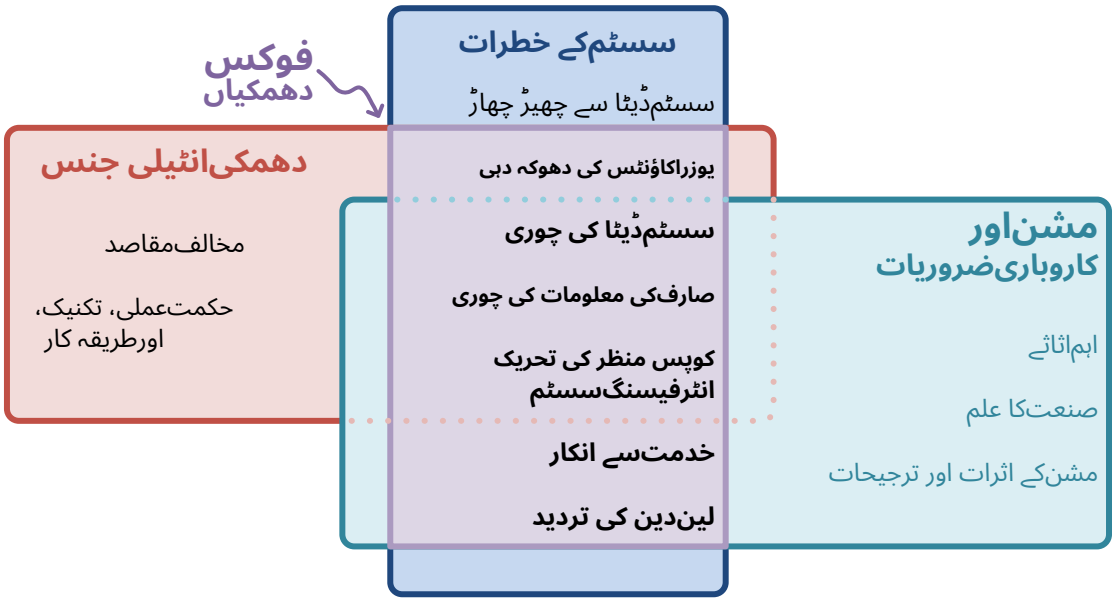
ایک‌منظم خطرے کے تجزیہ کے طریقہ کار کے بعد ڈیزائنرز کو نظام اور اس کے اثاثوں کے خلاف ممکنہ خطرات کی نشاندہی کرنے میں مددملتی ہے۔ یہ اس بات کا اندازہ کرنے کا ایک ذریعہ بھی فراہم کرتا ہے کہ کون سے کنٹرول اور ڈیزائن کے متبادل شناخت شدہ خطرات‌اور حملہ آوروں کو مؤثر طریقے سے کم کریں گے۔ مثال کے طور پر، باقی وقت میں ڈیٹا کی خفیہ کاری غیر مجاز انکشاف کو کم‌کر سکتی ہے، لیکن مخصوص عمل درآمد اس بات کا تعین کرتا ہے کہ یہ کس قسم کی چوری کے خلاف موثر ہو گی۔ یہ مثال کے طورپر، ڈسک کی سطح کی خفیہ کاری صرف جسمانی چوری کو کم کرتی ہے، جب کہ ایپلی کیشن کی سطح کی خفیہ کاری سسٹم کی‌سطح کے حملوں کو کم کرتی ہے۔ ہر آپشن سسٹم کی کارکردگی اور دیکھ بھال کی ضروریات کو مختلف طریقوں سے متاثر کرتا ہے۔یہ تجارت کی نمائندگی کرتے ہیں جو ڈیزائنر خطرات کو کم کرنے اور نظام کی دیگر ضروریات کے اثرات کو منظم کرنے میں کرتا ہے۔

یہاں‌تک کہ ایک ہلکے پیچیدہ نظام میں بھی بہت سے اثاثے ہوتے ہیں، اور اس وجہ سے بہت سے ممکنہ خطرات ہوتے ہیں۔ ڈیزائنرز تنظیم‌کے مشن اور کاروبار کی ضروریات کے بارے میں اپنی سمجھ کو بروئے کار لاتے ہیں تاکہ نظام کے خطرات کا اندازہ لگانے اور ان کی‌آزمائش میں مدد ملے۔ خطرے کی بالغ انٹیلی جنس پریکٹس والی تنظیمیں بھی اس معلومات کو سسٹم کے خطرے کے تجزیہ کےعمل میں شامل کرنے کے قابل ہیں۔ IDDIL/ATC طریقہ کار [6]، مثال کے طور پر، ایسے اقدامات فراہم کرتا ہے جو قدرتی طور پر مشن‌کی ضروریات اور خطرے کی ذہانت کو شامل کرتے ہیں۔ شکل 4 ان ان پٹ کو سسٹم کے خطرے کے تجزیہ کے عمل میں دکھاتاہے۔



تصویر4: سسٹم کے خطرے کے تجزیے میں مشن کی ضروریات اور خطرے کی ذہانت کو شامل کرنا

اس مشترکہ تجزیے کا استعمال کرتے ہوئے، ڈیزائنر ڈیزائن ٹریڈ آفس اور موثر سیکیورٹی کنٹرولز کے انتخاب کے بارے میں باخبر فیصلے کرنے کے قابل ہے۔ ڈیزائنرز کو احتیاط سے اندازہ لگانا چاہیے کہ وہ ہر خطرے کا مقابلہ کرنے کے لیے کس حد تک کنٹرول بناتے ہیں۔ مثال کے طور پر، جیسا کہ شکل 5 میں دکھایا گیا ہے، موجودہ خطرے کی انٹیلی جنس کی غیر موجودگی میں بھی نظام کے خلاف کچھ خطرات کو کم کیا جانا چاہیے، خاص طور پر جہاں نظام، مشن، یا تنظیم پر اثر شدید ہو۔



تصویر5: سسٹم کے خطرات، مشن کی ضروریات اور خطرے کی ذہانت کا استعمال

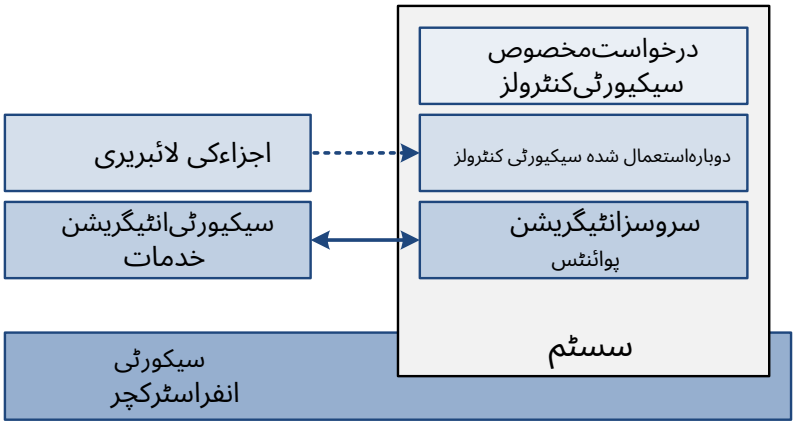
کنٹرولزکا انتخاب کرتے وقت، ڈیزائنرز نظام کے انفرادی خطرات اور مجموعی طور پر نظام کا فعال طور پر دفاع کرنے کی ضرورتدونوں پر توجہ دیتے ہیں۔ تنظیم کے سیکیورٹی کنٹرولز کا ایک کیٹلاگ جو شکل 6 میں بیان کردہ افعال کے سیٹ پر پھیلاہوا ہے اس بات کو یقینی بناتا ہے کہ ڈیزائنرز اپنے سسٹمز کے لیے دستیاب سیکیورٹی انفراسٹرکچر اور خدمات سے آگاہ ہیں۔کی بنیاد پر کنٹرول کی وضاحت کرتے ہوئے*افعال*وہ فراہم کرتے ہیں، یہ کیٹلاگ ڈیزائنرز کو واضح رہنمائی فراہم کرتا ہے کہ ہرکنٹرول سسٹم کو کیا فراہم کرتا ہے، بجائے اس کے کہ یہ کیا روکتا ہے۔ ڈیزائنرز بنیادی طور پر "پروٹیکٹ" فنکشنل گروپ میںسسٹم کے خطرات کو کم کرنے کے طور پر کنٹرولز کا فائدہ اٹھاتے ہیں، حالانکہ دوسرے فنکشنز کو پروٹیکٹ فنکشنز میں موجودخلا کو دور کرنے کے لیے معاوضہ کے کنٹرول کے طور پر لاگو کیا جا سکتا ہے۔

تاہم،نظام کے اثاثوں کے خلاف انفرادی خطرات کو مکمل طور پر کم کرنے سے ایک قابل دفاع نظام حاصل نہیں ہوتا ہے۔ جیساکہ سیکشن 3 میں بیان کیا گیا ہے، انٹیلی جنس پر مبنی دفاعی طریقوں کے لیے ڈیزائننگ کی ضرورت ہے۔*مرئیت* نظامکی سرگرمی اور رویے میں،*انتظامی صلاحیت*نئی انٹیلی جنس کی بنیاد پر سسٹم اپ ڈیٹس اور قواعد کی بروقت تعیناتیکے لیے، اور*بقا*حملے اور بحالی کے دوران خدمات فراہم کرنا جاری رکھنا۔ لہذا، ڈیزائنرز سسٹم میں قابل دفاع فن تعمیرکی خصوصیات کو بنانے کے لیے فنکشنل گروپس کی وسعت سے کنٹرول کا اطلاق کرتے ہیں۔ ذیل کے ذیلی حصے بیانکرتے ہیں کہ ان خصوصیات میں سے ہر ایک کو سسٹم کے ڈیزائن میں کیسے شامل کیا جائے۔

اختیار فنکشن	تفصیل			
انوینٹری	انکی زندگی بھر آئی ٹی اثاثوں کو دریافت کریں، ٹریک کریں اور رپورٹ کریں۔	✓	✓	
جمعکرنا	سسٹمکی سرگرمی کو پکڑیں، منظم کریں اور برقرار رکھیں	✓		
پتہلگانا	سسٹمکی سرگرمی کی شناخت اور انتباہ			✓
حفاظتکرنا	حملےاور غیر مجاز نظام کے رویے کو روکیں۔			✓
انتظامکریں۔	خطرےکی انٹیلی جنس کی بنیاد پر سسٹم کنفیگریشن، اپ ڈیٹس اور قواعد کو تعینات کریں۔		✓	
جواب دیں۔	واقعہسے نمٹنے، نظام کا تجزیہ، اور بحالی		✓	✓

تصویر6:فنکشنل کنٹرول کے درجہ بندی سے اعلی سطح کے کنٹرول کے افعال [6]

ایکتنظیم مختلف سطحوں پر اپنے کنٹرول فراہم کر سکتی ہے، جیسا کہ شکل 7 میں دکھایا گیا ہے۔ سیکیورٹی کا بنیادیڈھانچہ سسٹم کے ماحول میں بنائے گئے افعال پر مشتمل ہوتا ہے۔ مثالوں میں مکمل پیکٹ کیپچر اور نیٹ ورککرنٹمداخلت کا پتہ لگانا شامل ہے۔ سیکورٹی انضمام کی خدمات وہ ہیں جو نظام استعمال کر سکتا ہے، لیکن ان کےساتھ ضم ہونا ضروری ہے۔ مثالوں میں لاگ جمع کرنا اور تصدیق کی خدمات شامل ہیں۔ دوبارہ استعمال شدہ سیکیورٹیکنٹرولز کو نظم شدہ لائبریریوں، جیسے آپریٹنگ سسٹم کی تصاویر اور کرپٹوگرافی لائبریریوں سے سسٹم میںتعینات کیا جاتا ہے۔ آخر میں، ایپلیکیشن کے لیے مخصوص سیکیورٹی کنٹرولز وہ ہیں جو ایک ایپلیکیشن کو خود ہیلاگو کرنا چاہیے، جیسے کہ ان پٹ کی توثیق، میموری چیک، اور ایپلیکیشن ایونٹ لاگ۔ ڈیزائنرز جہاں ممکن ہو انفراسٹرکچراور خدمات کا استعمال کرتے ہیں، جس سے سسٹم کے ڈویلپرز اور ایڈمنسٹریٹرز سسٹم کی بنیادی فعالیتپر توجہ مرکوز کر سکتے ہیں۔ یہ کنٹرولز کے مزید مستقل نفاذ کی طرف بھی جاتا ہے اور بنیادی ڈھانچے کی عام تہپر مرئیت فراہم کرکے مجموعی دفاع کو بہتر بناتا ہے۔



تصویر7:دستیاب سیکیورٹی کنٹرول کے درجات

4.1.1مرئیت کے لیے ڈیزائننگ

مرئیت کے لیے ڈیزائن کرنے کا مقصد محافظوں کو نظام کے اندر موجودہ اور تاریخی سرگرمیوں کی جامع نگرانی کرنے کے قابل بنانا ہے۔ مرئیت کے کنٹرول منتظمین اور محافظوں کو وقت کے ساتھ ساتھ اور نظام کے تمام اجزاء کے ساتھ واقعات کی ترتیب کو دوبارہ بنانے کی اجازت دیتے ہیں۔ اس کے لیے نظام کے اندر اہم مقامات پر مرئیت کے کنٹرول کو رکھنے کی ضرورت ہے۔ اس کا مطلب یہ بھی ہے کہ ریکارڈ شدہ واقعات کے مواد میں وقت کے ساتھ ساتھ اور تمام اجزاء کے ساتھ لاگ اندراجات کو باہم مربوط کرنے کے لیے کافی معلومات ہونی چاہیے۔ شکل 8 سوالات اور سرگرمیوں کا ایک نمونہ فراہم کرتا ہے جن پر ڈیزائنر مرئیت کی ضروریات کا تعین کرتے وقت غور کرتا ہے۔

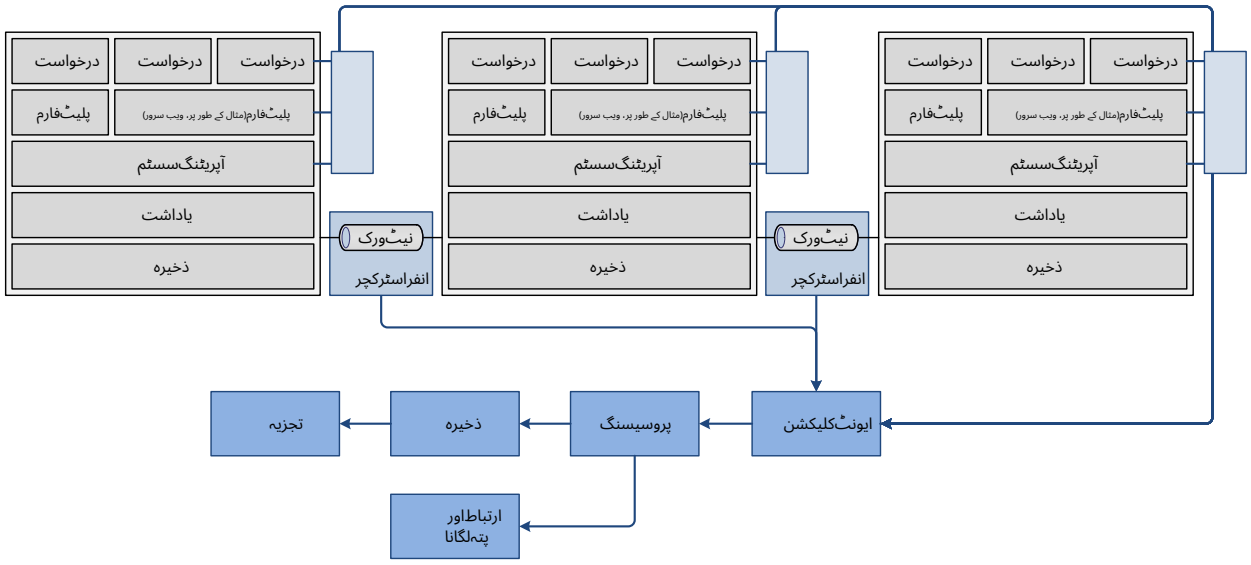
نیٹ ورک	کیا بات کرتا ہے، کب؟
	مجھے وہ سب کچھ دکھائیں جو نیٹ ورک پر چلا گیا تھا۔
	اگر مواصلات کو خفیہ کیا جائے تو کیا ہوگا؟
	مجھے بتائیں کہ کیا معلوم بدنیتی پر مبنی ٹریفک نیٹ ورک پر جاتا ہے۔
آپریٹنگ سسٹمز	سرور / ورک سٹیشن پر کیا ہو رہا ہے؟
	مجھے بتائیں کہ جب کوئی معلوم نقصان دہ ہوتا ہے۔
	ہر سسٹم پر کیا انسٹال اور پیچ کیا گیا ہے؟
	مجھے دیئے گئے نظام کی فرانزک تصویر کی ضرورت ہے۔
پلیٹ فارم اور درخواست	ویب سرور، ڈی بی ایم ایس، ایپلیکیشن وغیرہ پر کیا ہو رہا ہے؟
	نظام کے اندر اور باہر کیا جا رہا ہے؟
	صارف نے سسٹم میں کیا کرنے کی کوشش کی؟
	کون سے نیٹ ورک اور OS ایونٹس صارف کے اس عمل سے مطابقت رکھتے ہیں؟
شناخت& رسائی انتظام	کون سے اکاؤنٹس کہاں، کب اور کس کے ذریعے بنائے گئے؟
	کس نے، کب، کہاں اور کیسے تصدیق کی؟
	صارف نے کون سے مجاز اعمال انجام دیے؟
	صارف نے کون سے غیر مجاز اقدامات کی کوشش کی؟

تصویر8:نظام کی مختلف پرتوں پر مرئیت کے مقاصد کا نمونہ

سسٹم کے مجموعی فن تعمیر کے لیے استعمال ہونے والے سسٹم کے خطرے کا تجزیہ بھی اس بات کا تعین کرنے میں استعمال ہوتا ہے کہ سسٹم میں مرئیت کے کنٹرول کو کہاں تلاش کرنا ہے۔ خطرے کے ماڈل میں اعتماد کی حدود سسٹم میں لاگو کرنے کے لیے اہم دفاعی خطوط کی نمائندگی کرتی ہیں۔ اعتماد کی حدود اور نظام کے اثاثوں پر سرگرمی کی نگرانی منتظمین کو قیمتی تشخیصی معلومات فراہم کرتی ہے، اور محافظوں کو مخالف سرگرمی میں ضروری مرئیت فراہم کرتی ہے۔ ممکنہ حد تک، ڈیزائنرز سسٹم کے ماحول اور سسٹم کے لیے دستیاب انٹیگریشن سروسز میں بنائے گئے مرئیت کے بنیادی ڈھانچے کا فائدہ اٹھاتے ہیں۔

مرئیت کے حقیقی وقت اور تاریخی استعمال دونوں کو دیکھتے ہوئے، واقعہ جمع کرنے، پتہ لگانے، ذخیرہ کرنے اور تجزیہ کرنے کے تصورات کو الگ کرنا ضروری ہے۔ نیٹ ورک ڈیٹا اور سسٹم لاگز کو جمع کرنے کے عمل بعد میں پروسیسنگ، اسٹوریج اور تجزیہ کے ساتھ ارتباط اور پتہ لگانے کے طریقہ کار کو فیڈ کر سکتے ہیں، جیسا کہ

تصویر9 میں دکھایا گیا ہے۔ پورے انٹرپرائز میں مجموعی طور پر مرئیت کے لیے ڈیزائننگ اس بات کو یقینی بناتی ہے کہ حملے کی اہم‌سطحوں کی نگرانی کی جائے اور مختلف سینسرز سے جمع کیے گئے ڈیٹا کو آپس میں جوڑا اور اس پر محور کیا جا سکے۔ Defendable Enterprise میں مجموعی مرئیت کے بارے میں مزید معلومات کے لیے سیکشن 5 دیکھیں۔



تصویر9:مرئیت کا بنیادی ڈھانچہ

مرئیت‌کے اعداد و شمار کو جمع کرنا اور ذخیرہ کرنا کسی تنظیم کے کمپیوٹنگ، نیٹ ورک، اور ذخیرہ کرنے کی صلاحیت پر مطالبہ‌کرتا ہے۔ ڈیزائنرز، منتظمین، اور محافظ مرئیت کے مقامات، جمع کرنے کی شرحوں، اور برقرار رکھنے کی مدت کو ترجیح‌دینے کے لیے تعاون کرتے ہیں۔ عام طور پر مرئیت کے تقاضے نیٹ ورک کی پرت سے شروع ہوتے ہیں، اور پھر اسٹیک کو آپریٹنگ‌سسٹمز اور ایپلیکیشنز میں لے جاتے ہیں۔ اس کے بعد کی ہر پرت جمع کیے جانے والے واقعات کے سیمنٹکس کو تقویت‌دیتی ہے، لیکن اعداد و شمار کو معمول پر لانے میں حجم اور چیلنجز کو بھی شامل کرتی ہے۔ انتہائی متنوع مرئی ذرائع،جیسے ایپلیکیشن لاگز اکثر خود کو معمول پر لانے کے لیے اچھی طرح سے قرض نہیں دیتے ہیں۔ تجزیہ کے دوران پروسیسنگ‌کے لیے ان لاگز کو نسبتاً خام شکل میں چھوڑنا اکثر بہتر ہوتا ہے۔

مرئیت‌فعال حملوں کی نگرانی سے باہر ہوتی ہے۔ مثال کے طور پر، یہ جاننا کہ ایک مخالف کب اور کیسے جاسوسی کر رہاہے، اور اس سرگرمی کو حملے کے بعد کے مراحل سے جوڑنے کے قابل ہونا، اس بارے میں اہم ذہانت فراہم کرتا ہے کہ کوئی‌خاص مخالف کیسے کام کرتا ہے۔ ایک ڈیزائنر کے طور پر، اس بات سے آگاہ ہونا کہ حملے کے ہر مرحلے میں کس طرح‌سسٹم کا غلط استعمال کیا جا سکتا ہے اور اس سرگرمی میں مرئیت کو یقینی بنانا ڈیفنڈ ایبل آرکیٹیکچرز کی تعمیرکے اہم حصے ہیں۔

4.1.2انتظام کے لیے ڈیزائننگ

ایک‌قابل انتظام نظام وہ ہے جس کا موجودہ اور ابھرتے ہوئے حملوں کے خلاف فعال طور پر دفاع کیا جا سکتا ہے، جس کے لیے ایک ایسےڈیزائن کی ضرورت ہوتی ہے جو بنیادی انوینٹری، کنفیگریشن، اور خطرے کے انتظام کے ساتھ ساتھ خطرے کی انٹیلی جنس سےاخذ کردہ اشارے، TTPs، اور مخالف مقاصد پر مبنی کنٹرولز کے لیے فوری اپ ڈیٹس کی حمایت کرتا ہو۔

کمزوری‌کے انتظام کے لیے سسٹم کے تمام اجزاء کی بروقت پیچنگ اور کنفیگریشن کی ضرورت ہوتی ہے۔ اگرچہ بنیادی ڈھانچےکو پیچ کرنے سے اس کی زیادہ تر ضرورت کو پورا کیا جا سکتا ہے، ڈیزائنرز کو یہ تسلیم کرنا چاہیے کہ کچھ اجزاء انٹرپرائزپیچنگ سسٹم کے ذریعے آسانی سے تعاون یافتہ نہیں ہیں۔ ان اجزاء کے لیے عام طور پر منتظمین کو دستی طور پر پیچ‌ڈاؤن لوڈ کرنے اور لاگو کرنے کی ضرورت ہوتی ہے۔ توسیع کے لحاظ سے، محض پیچنگ سافٹ ویئر اسے محفوظ نہیں بناتاہے۔ منتظمین کو بھی اس کی ترتیب ترتیب اور برقرار رکھنی چاہیے۔ جیسا کہ پیچنگ کے ساتھ، کنفیگریشن مینجمنٹ اس‌مسئلے کے سیٹ سے بہت زیادہ، لیکن تمام نہیں، حل کرتی ہے۔

لہذا،انتظام کے لیے ڈیزائننگ میں منتظمین کے لیے اجزاء کو دستی طور پر انسٹال، پیچ اور ترتیب دینے کا طریقہ کار بھی‌شامل ہے۔ ڈیفنڈ ایبل آرکیٹیکچر میں منتظمین کے لیے سسٹمز تک رسائی، اپ ڈیٹس ڈاؤن لوڈ، اور سسٹم کنفیگریشن‌کا نظم کرنے کے لیے کنٹرول شدہ اور نگرانی شدہ راستے شامل ہیں۔ دی

مرئیت‌اور بقا کی خصوصیات کا اطلاق انتظامیہ کے راستوں پر بھی ہوتا ہے۔ ایڈمنسٹریٹر انٹرفیس پر سرگرمی کی نگرانی‌کرنا اس بات کی بصیرت فراہم کرتا ہے کہ کون سے اقدامات کب، کس کے ذریعے اور کہاں سے کیے گئے۔ واقعہ سےواقعات کی ترتیب کو دوبارہ بنانے کے لیے ضروری ہے۔ بقا اس بات کو یقینی بناتی ہے کہ منتظمین اب بھی نظام کو منظم‌کرنے کے قابل ہوں گے، یہاں تک کہ جب یہ حملہ آور ہو۔

متضادطور پر، بہت سے انتظامی افعال اضافی بیرونی انٹرفیس کی ضرورت کے ذریعے سسٹم کے حملے کی سطح کو بڑھاسکتے ہیں۔ ان افعال کے لیے ہر ایک کے نفاذ کی ضرورت اور ذرائع کو نظام اور اس کے خطرات کے تناظر میں سمجھاجانا چاہیے۔ مثال کے طور پر، زیادہ تر معاملات میں پیچنگ کو سپورٹ کرنے کے لیے ایک خودکار انٹرفیس ایک مناسب‌نفاذ ہے۔ تاہم، کچھ منظرناموں میں، جیسے کہ ایئر گیپڈ سسٹم، پیچنگ فریکوئنسی کو کم کرنا درحقیقت مجموعی‌نظام کے خطرے کو کم کر سکتا ہے، یہ فرض کرتے ہوئے کہ معاوضہ دینے والے کنٹرول موجود ہیں۔

نظم‌و نسق کے لیے ڈیزائننگ کا دوسرا حصہ سسٹم کے سیکیورٹی کنٹرولز میں نئے خطرے کی انٹیلی جنس کو شامل کرناہے۔ جو تنظیمیں ایسا کرتی ہیں وہ اپنے سائبر سیکیورٹی دفاع میں اپنے آپ کو کلاسیکی سیکیورٹی اصولوں پر مبنی‌اداروں سے ممتاز کرتی ہیں۔ ڈیفنڈ ایبل آرکیٹیکچرز پر مبنی سسٹمز انتظامی قابلیت کے اس حصے کو حاصل کر سکتےہیں اگرچہ عام سیکورٹی انفراسٹرکچر اور خدمات کا استعمال کرتے ہوئے جو سسٹم کے فن تعمیر میں ہر پرت پر لاگوہوتے ہیں۔

اس‌کا مطلب ہے کہ نیٹ ورک، آپریٹنگ سسٹم، پلیٹ فارم، اور ایپلیکیشن لیئرز پر کنٹرول ہونا۔ یہ محافظوں کو سسٹم‌کے اسٹیک کی مناسب سطح پر کنٹرولز کو اپ ڈیٹ کرنے کی اجازت دیتا ہے۔ مثال کے طور پر، کسی مخالف کے بنیادی‌ڈھانچے کے بارے میں انٹیلی جنس کچھ IP پتوں کو بلاک کرنے کے اشارے حاصل کر سکتی ہے، اور اسے IP فائر وال‌میں لاگو کیا جا سکتا ہے۔ جبکہ کمانڈ اینڈ کنٹرول پروٹوکول کے بارے میں انٹیلی جنس HTTP ہیڈر اور مواد کی بنیادپر قواعد حاصل کر سکتی ہے، اور اسے ویب پراکسی میں لاگو کیا جا سکتا ہے۔ سسٹم میں مختلف پرتوں پر اور متعددسسٹمز پر کنٹرولز کو اپ ڈیٹ کرنے کی یہ صلاحیت، محافظوں کو درست طریقے سے بنائے گئے اصولوں کو نافذکرنے کی اجازت دیتی ہے، جو موجودہ اور ابھرتے ہوئے حملوں کے خلاف تعینات کنٹرولز کی افادیت کو بہت بہتر بناتی‌ہے۔ کسی تنظیم کے کنٹرول کے کیٹلاگ کے درمیان ایک کراس حوالہ، جیسا کہ [6] میں بیان کردہ اشارے کی اقسام‌کے ساتھ جن کو ہر کنٹرول مؤثر طریقے سے کم کر سکتا ہے، ڈیزائنرز اور محافظ دونوں کو اہم بصیرت فراہم کرتا ہے۔

پروٹیکشن‌کنٹرولز کے ساتھ مرئیت کے وینٹیج پوائنٹس کو سیدھ میں لا کر، محافظ تاریخی نیٹ ورک ٹریفک اور سسٹم لاگز کی بنیادپر قواعد کی جانچ اور ٹیوننگ کرنے کے قابل ہوتے ہیں۔ یہ محافظوں کو اعتماد کے ساتھ نئے اور اپ ڈیٹ کردہ قوانین کو غلط مثبت‌یا غیر ارادی کاروباری اثرات کے کم خطرے کے ساتھ تعینات کرنے کی اجازت دیتا ہے۔ مزید برآں، ڈیفنڈ ایبل آرکیٹیکچرز پر مبنی‌انفراسٹرکچر کو ٹی ٹی پی میں تبدیلیوں اور حتیٰ کہ مخالف مقاصد کے لیے بھی ڈھال لیا جا سکتا ہے۔ موجودہ مرئیت جمع کرنےکی صلاحیتوں کے اوپر عمارت کا تحفظ ایک لچکدار فن تعمیر فراہم کرتا ہے جو کہ موجودہ ڈیٹا اکٹھا کرنے کی پائپ لائن کی بنیادپر نئے قسم کے قواعد اور بلاک کرنے کی تکنیکوں کو شامل کرنے کو ہموار کرتا ہے، جس سے دفاعی چستی میں اضافہ ہوتا ہے۔

اس‌لحاظ سے، قابل دفاع آرکیٹیکچرز گہرائی میں دفاع کے کلاسیکی نقطہ نظر سے الگ ہیں، اگرچہ باہمی طور پر الگ نہیں ہیں۔روایتی طور پر، گہرائی میں دفاع اس خیال کو فروغ دیتا ہے کہ ایک جیسے مقصد کے ساتھ متعدد کنٹرولز ایک دوسرے کی‌کمزوریوں کو دور کر دیں گے، کنٹرولز کو فلٹرز کے ایک جامد جھرنے کے طور پر پیش کرتے ہوئے اس توقع میں کہ کم از کم ایک‌کے پاس حملے کو روکنے کے لیے درست ترتیب ہو گی۔ تاہم، گہرائی میں دفاع کی طرف سے مسلط کردہ تفاوت ایک نظام کی‌انتظامی صلاحیت کو کم کر دیتا ہے کیونکہ منتظمین کو متعدد ٹولز میں مہارت حاصل کرنے اور ان کو برقرار رکھنے میں وقت‌گزارنے کی ضرورت ہوتی ہے۔ ڈیفنڈ ایبل آرکیٹیکچرز ایسے سسٹم بنانے پر توجہ مرکوز کرتے ہیں جو خطرے کی ذہانت اور سسٹم‌کے خطرے کے تجزیے کی بنیاد پر سسٹم کے اسٹیک پر فعال طور پر ٹیوننڈ کنٹرولز کو لاگو کر سکتے ہیں۔

4.1.3بقا کے لیے ڈیزائننگ

زندہ‌رہنے کی صلاحیت حملے، سمجھوتہ اور بحالی کے دوران نظام کی اپنی مطلوبہ خدمت فراہم کرنے کی صلاحیت ہے۔ ایک‌مخالف کے مقاصد بقا کے طریقہ کار کی اقسام کو متاثر کرتے ہیں جو ایک نظام میں ہونے چاہئیں۔ حملہ آور جن کا مقصدکمپیوٹر نیٹ ورک ایکسپلائیٹیشن (CNE) ہے ان کا مقصد ہدف شدہ تنظیم سے معلومات نکالنا ہے۔ اس صورت‌میں، نظام کا سمجھوتہ شاذ و نادر ہی نظام کے ناکام ہونے کا سبب بنتا ہے۔ گھسنے والے کے مقصد کا ایک حصہ ناقابل‌شناخت رہنا ہے، اور بہت سے حملہ آور بچنے کے لیے کافی حد تک چلے جاتے ہیں

پتہ‌لگانے CNE کے معاملے میں، یہ دریافت اور بحالی کا عمل ہے – ابتدائی سمجھوتہ نہیں – جو نظام کے لیے سب سے زیادہ‌خلل ڈالتا ہے۔ ایک بار کامیاب حملے کا پتہ چلنے کے بعد، تجزیہ اور بحالی کے لیے سسٹم کو آف لائن لے کر تنظیمیں اکثرناکامی کا باعث بنتی ہیں۔

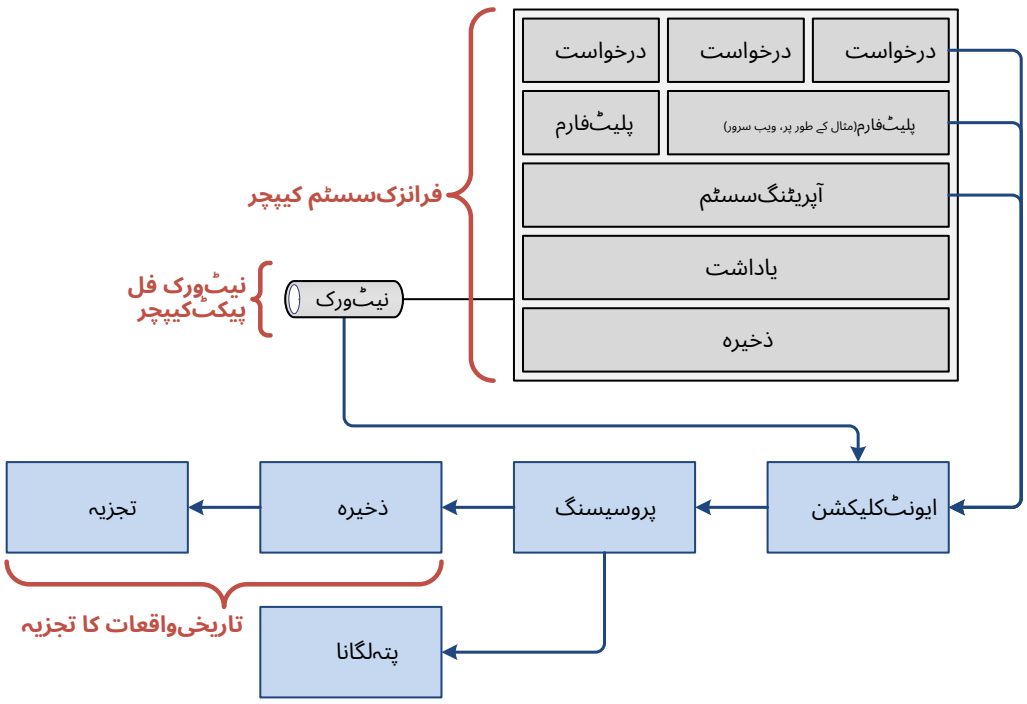
کےلیے ہدف بنائے گئے ہیں۔ CNE حملے میں۔ تاہم، اکثر سی این اے کی ترتیب ایسے نظاموں تک ناقابل شناخت رسائی حاصل‌کرنے سے شروع ہوتی ہے جو بعد میں پس منظر کی حرکت کے ذریعے ہدف تک رسائی فراہم کرتے ہیں۔ اس اٹیک ویکٹرپر سسٹمز زندہ رہنے کی انہی ضروریات کے تابع ہیں جو)DOS(ہے وہ کسی تنظیم کے اثاثوں کے کچھ حصوں میں خلل‌ڈالنے یا تباہ کرنے کا ارادہ رکھتے ہیں۔ بعض صورتوں میں، حملے کے تحت نظام ہدف ہوتا ہے، جیسے سروس سے انکار)CNA(کے برعکس، حملہ آور جن کا ہدف کمپیوٹر نیٹ ورک اٹیک CNE

سی‌این ای اور سی این اے دونوں کے معاملے میں، سسٹم ڈیزائنرز کو سسٹم کے خطرے کے تجزیے کے نمونے کا موازنہ مخالفوں‌کے مقاصد کے بارے میں دستیاب خطرے کی انٹیلی جنس کے ساتھ کرنا چاہیے، جیسا کہ سیکشن 4.1 میں بیان کیاگیا ہے۔ یہ ڈیزائنر کو دفاعی اقدامات کا انتخاب کرنے کی اجازت دیتا ہے جو نظام کی متوقع حملوں کے مقاصد اور نظام کی کاروباری‌تنقید کے ساتھ مل کر نظام کی ضروریات کو پورا کرتا ہے۔ مخالف مقاصد کو تبدیل کرنے سے سسٹم کے ڈیزائن یا معاون‌کنٹرول میں تبدیلی کی ضرورت پڑ سکتی ہے۔ مثال کے طور پر، نئی تھریٹ انٹیلی جنس جو اس بات کی نشاندہی کرتی‌ہے کہ کسی سسٹم کو ڈیٹا سے چھیڑ چھاڑ کے لیے نشانہ بنایا جا سکتا ہے، نظام میں عمدہ آڈیٹنگ اور انٹیگریٹی کنٹرول کےنفاذ کو ترجیح دے گا۔ خطرے کے تجزیہ کی تکنیک کا استعمال کرتے ہوئے ڈیزائن کے مرحلے کے دوران ان ضروریات کا اندازہ‌لگایا جا سکتا ہے۔ یہاں تک کہ جہاں کنٹرول سسٹم کے ابتدائی نفاذ میں نہیں بنائے گئے ہیں، انہیں مستقبل کے انضمام کےلیے ڈیزائن کیا جا سکتا ہے۔

واقعہ‌کی بازیابی کا سب سے عام ردعمل پورے سسٹم کو آف لائن لے جانا، سسٹم پر فرانزک تجزیہ کرنا ہے تاکہ یہ سمجھ‌سکیں کہ کب، کیسے، اور کن پرزوں سے سمجھوتہ کیا گیا ہے، پھر بیک اپ یا تعمیراتی طریقہ کار سے سسٹم کی‌ترتیب اور ڈیٹا کو بحال کرنا ہے۔ اگرچہ یہ ڈیزائن اور آپریشنل اپروچ بہت سے سسٹمز کے لیے قابل قبول ہے، لیکن مشنکریٹیکل‌سسٹمز کے لیے بہت زیادہ نفیس انداز کی ضرورت ہے۔

ایک‌زیادہ جدید زندہ رہنے کے قابل ڈیزائن نظام کو تجزیہ اور بحالی کے دوران کام جاری رکھنے کی اجازت دے گا۔ بحالی کےدوران کام میں رہنے کی اہلیت اس فن تعمیر پر منحصر ہے جو (1) سسٹم کے اجزاء کی موجودہ اور تاریخی حالت میں‌مکمل مرئیت اور تجزیہ فراہم کرتا ہے، (2) اجزاء کو آف لائن لے جانے اور معمول کے آپریشن کو متاثر کیے بغیر واپس‌آن لائن رکھنے کی اجازت دیتا ہے۔ .

اس‌معاملے میں مرئیت اوپر بیان کردہ خصوصیت کی توسیع ہے۔ حملہ آور کی سرگرمی کی دریافت اور تجزیہ کی حمایت‌کرنے کے لیے، مرئیت کو سسٹم اسٹیک کی گہرائی، اور ایپلی‌کیشن کے تمام اجزاء میں وسعت کا احاطہ کرنا چاہیے۔اس میں وقت کے ڈومین کا دورانیہ بھی ہونا چاہیے، آن ڈیمانڈ فرانزک کیپچر سے لے کر سسٹم میں تاریخی سرگرمی‌تک۔ ان میں نیٹ ورک ٹریفک کیپچر، فائل سسٹمز میں لاگنگ تبدیلیاں، آپریٹنگ سسٹم، ایپلیکیشن کنفیگریشن،اور ایپلیکیشن کی سرگرمی شامل ہوگی۔ آخر میں، اسے سسٹم اسٹیٹ کی مکمل فرانزک کیپچر کرنے کی صلاحیت‌کی ضرورت ہوتی ہے، بشمول میموری اور نیٹ ورک ٹریفک۔ یہ مداخلت کے تجزیہ کاروں کے لیے ضروری ہیں کہ‌وہ نظام کی موجودہ حالت کا جائزہ لیں اور دوسرے ذرائع سے اشارے اور مہم کی انٹیلی جنس کے ساتھ ہم آہنگ ہوں۔اس تجزیے کی بنیاد پر، یہ طے کرنا ممکن ہے کہ کن اجزاء سے سمجھوتہ کیا گیا ہے اور کتنے عرصے تک۔ اس کے بعد سسٹم‌کے بیک اپ، تعمیراتی طریقہ کار، اور ٹیسٹ پلانز کی بنیاد پر ایک یقینی وصولی کی جا سکتی ہے۔



تصویر10:دخل اندازی کے تجزیہ اور بازیابی کے لیے مرئیت

زندہ‌رہنے کے قابل جدید ڈیزائنز کی دوسری ضرورت - اجزاء کو آف لائن لے جانے اور آن لائن واپس رکھنے کی اجازت دینا -اجزاء کی ناکامی کے لیے ڈیزائن کرنے کی ضرورت ہے۔ اجزاء کی ناکامی کو سہارا دینے کے لیے کئی ڈیزائن پیٹرن موجود ہیں،اور بہت سے جدید نظام کے فن تعمیرات کو انفرادی اجزاء کی ناکامی کو خوبصورتی سے برداشت کرنے کے لیے ڈیزائن‌کیا گیا ہے۔ یہ نظام کو نظام کے حصوں کے خلاف دستیابی کے نقصان سے بچنے کی اجازت دیتا ہے، چاہے حادثاتی (مثلاً،سسٹم کریش) یا جان بوجھ کر (مثلاً، سروس حملے سے انکار)۔ افراتفری بندر [7] واضح طور پر ڈیزائن اور اجزاء کی‌ناکامی کے لیے تعمیر کی ایک بہترین مثال ہے۔ جان بوجھ کر اجزاء کو ڈیزائن کرنے سے – اور مسلسل ناکامی کا شکار ہونے‌سے، ایک مجموعی نظام دستیابی کی خرابیوں کے لیے انتہائی لچکدار ہو سکتا ہے۔ ڈیزائنرز پورے نظام کی مجموعی بقاکو سمجھنے کے لیے ناکامی یا سمجھوتہ کے واحد نکات کے لیے نظام کا جائزہ لیتے ہیں۔

اجزاءکی ناکامی کے لیے ڈیزائننگ صرف دستیابی کے نقصان کو دور کرتی ہے۔ یہ حملے کی وجہ سے سسٹم کے اجزاء کے سمجھوتہ‌کو مناسب طریقے سے حل نہیں کرتا ہے۔ اس صورت میں، ڈیزائنرز بھی ایک جزو کے قابل اعتماد پر غور کرتے ہیں. CNE اور CNA دونوں میں، انفرادی اجزاء چلتے رہ سکتے ہیں، لیکن اپنے کام کو صحیح طریقے سے انجام دینے پر بھروسہ نہیں‌کیا جا سکتا ہے۔ سسٹم کو اس لیے ڈیزائن کیا گیا ہے کہ منتظمین کو نظام میں اجزاء کی قابل اعتماد حیثیت کو منتخب‌طور پر تبدیل کر سکیں۔ کچھ ڈیزائنز کے لیے، یہ انفراسٹرکچر کنٹرولز جیسے کہ سروس اکاؤنٹس کو غیر فعال کرنا یا نیٹ‌ورک آئسولیشن کا استعمال کرتے ہوئے پورا کیا جا سکتا ہے۔ دیگر سسٹمز کو گرانولریٹی کی ضروری ڈگری حاصل کرنے کےلیے ایپلیکیشن لیول کنٹرولز کی ضرورت ہوتی ہے۔

4.1.3.1پس منظر کی حرکت

بہت‌سے حملہ آور ابتدائی طور پر سمجھوتہ کرنے والے نظام کو ایک قدم کے طور پر استعمال کرتے ہیں تاکہ نظام کے اندر اور اس کے درمیان دیرسے منتقل ہو سکیں۔ یہ ایک حملہ آور کو انٹرپرائز کے اندر اپنی رسائی کا دائرہ وسیع کرنے اور ابتدائی داخلے کے لیے کمزور اہداف کا انتخاب‌کرنے کی اجازت دیتا ہے۔

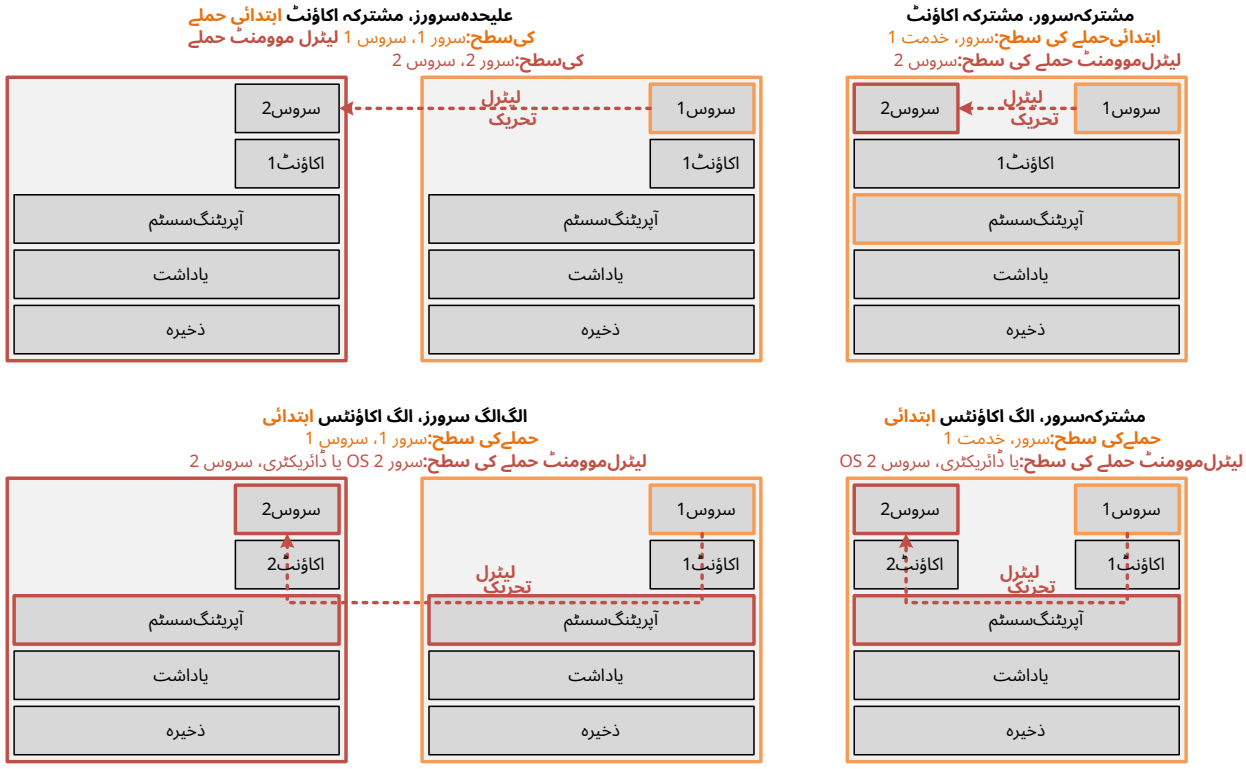
مداخلت‌سے خوبصورتی سے بازیافت کرنے کے قابل ہونے کے علاوہ، ایک زندہ رہنے والا نظام ابتدائی سمجھوتہ پر مشتمل‌کرنے کے لیے ڈیزائن کیا گیا ہے۔ پس منظر کی نقل و حرکت کا مطلب یہ ہے کہ ڈیزائنرز سسٹم کے اندر اعتماد کی‌حدود کی مزید جانچ پڑتال کرتے ہیں۔ اجزاء کے درمیان بہت کم انٹرفیس کو مکمل طور پر قابل اعتماد سمجھا جانا چاہئے۔انٹرفیسنگ اجزاء کیا ہیں اس کی واضح تفہیم*قابل*ایک دوسرے کے ساتھ کرنا -

بجائےاس کے کہ وہ کیا ہیں۔*ارادہ کیا*کرنا - پس منظر کی نقل و حرکت کو مناسب طریقے سے کم کرنے کے لیے ضروری ہے۔

پس‌منظر کی نقل و حرکت کا اندازہ کرتے وقت، ڈیزائنرز ایسے اجزاء پر غور کرتے ہیں جو عام طور پر ایک دوسرے کے ساتھ انٹرفیس‌نہیں کرتے ہیں، لیکن یہ بھی نہیں ہیں*روکا*انٹرفیسنگ سے. یہ ہوسٹنگ ماحول میں پڑوسی نظاموں کے ساتھ ایک عام‌مسئلہ ہے۔ یہاں تک کہ اگر وہ انٹرفیس کے لیے ڈیزائن نہیں کیے گئے ہیں، تو ملحقہ نظاموں کا مضمر اعتماد حملہ آور کو براہ‌راست روابط قائم کرنے کی اجازت دے سکتا ہے، یا عام انفراسٹرکچر جیسے کہ تصدیق یا بیک اپ سروسز کے ذریعے۔ تھریٹ‌انٹیلیجنس عام طور پر استعمال ہونے والی لیٹرل موومنٹ TTPs کے بارے میں بصیرت فراہم کر سکتی ہے، جو ڈیزائنرزکو معاوضہ دینے والے کنٹرول کو ترجیح دینے میں مدد کرتی ہے۔

پس‌منظر کی نقل و حرکت کے خلاف مزاحمت روایتی نظام کی سختی اور نظاموں کے درمیان حملے کی سطح کو محدود کرنے کے لیےکم از کم استحقاق کی ترتیب سے شروع ہوتی ہے۔ تاہم، قابل دفاع آرکیٹیکچرز لاگنگ اور نیٹ ورک کی نگرانی کے ذریعے پس منظرکی نقل و حرکت میں مرئیت کو بھی یقینی بناتے ہیں۔

نظام‌کی تقسیم کے بارے میں ڈیزائن کے فیصلے بقا کو بہت زیادہ متاثر کر سکتے ہیں۔ جوڑے اور ہم آہنگی کے بنیادی ڈیزائن‌کے اصول پس منظر کی نقل و حرکت کے خلاف نظام کی مزاحمت پر گہرا اثر رکھتے ہیں۔ مضبوطی سے جوڑے جانےوالے اجزاء اعلی درجے کے اعتماد کا اشتراک کرتے ہیں، جس کا پس منظرکی نقل و حرکت کے لیے فائدہ اٹھانا آسان‌ہے۔ دو سافٹ ویئر سروسز کو چلانے کے لیے، شکل 11 میں دکھائے گئے ڈیزائن کے متبادل پر غور کریں۔ ڈیزائن کے اختیارات‌کا ایک آسان سیٹ بیلنس شیئرنگ اکاؤنٹس اور سرورز۔ کنفیگریشن A میں، سروسز آپریٹنگ سسٹم اور سروس‌اکاؤنٹ کے ذریعے مضبوطی سے جوڑے جاتے ہیں اور اعتماد کا اشتراک کرتے ہیں۔ سروس خود ایک حملہ آور کے خلاف‌واحد دفاعی حد ہے جس نے دوسری سروس پر کنٹرول حاصل کر لیا ہے۔ دوسری انتہا پر، کنفیگریشن D الگ الگ اکاؤنٹس‌اور الگ سرورز کا استعمال کرتی ہے، جو حملہ آور کو دوسرے اکاؤنٹ اور دوسرے سرور سے سمجھوتہ کرنے پر مجبورکرتی ہے۔



تصویر11:مختلف اجزاء کی تقسیم کے اختیارات میں ظاہری حملے کی سطحوں کا موازنہ

تجزیہ‌کرنے سے کہ کس طرح، اور کس حد تک، حملے کی سطح کا دفاع کیا جا سکتا ہے، ڈیزائنرز کو سسٹم کی ترتیب کےبارے میں باخبر فیصلے کرنے میں مدد کرتا ہے۔ حملہ کرنے والی سطحوں پر مرئیت اور بقاء فراہم کرنے کے طریقے پر غورکرکے، ڈیزائنرز نظام اور ڈگری کے اندر تقسیم کی مناسب شکلوں کا تعین کر سکتے ہیں۔

جس‌پر انفرادی اجزاء پر بھروسہ کیا جا سکتا ہے۔ ڈیزائنر ان اختیارات کو سسٹم کے خلاف خطرات، پس منظر کی نقل وحرکت کے بارے میں خطرے کی ذہانت، اور نظام پر انتظامی رکاوٹوں کے خلاف وزن کرتا ہے۔ جیسا کہ زیادہ تر ڈیزائن کےفیصلوں کے ساتھ، نظام کی فعالیت، سیکورٹی، اور آپریشنل اخراجات پر اثرات پر غور کرنے کے لیے ان تجارتوں کو مجموعی‌طور پر لیا جانا چاہیے۔

4.2قابل دفاع نظام بنانا

ڈیولپرز،انجینئرز، اور ٹیسٹرز سسٹمز میں دفاعی اقدامات کو نافذ کرنے اور ان کو مربوط کرنے کے ذمہ دار ہیں۔ ڈیزائنرز کی‌طرف سے سسٹم کے خطرے کے تجزیے اور محافظوں سے خطرے کی ذہانت کا فائدہ اٹھاتے ہوئے، ڈویلپرز درست کنٹرول‌کے نفاذ کا انتخاب کرتے ہیں، اور ٹیسٹرز حقیقی دنیا کے حملوں کی بنیاد پر تصدیق کے طریقوں کو ترجیح دیتے ہیں۔

جیساکہ ڈیزائنرز کے ساتھ ہے، سسٹم کے ڈویلپرز اور ٹیسٹرز کو دستیاب سیکیورٹی انفراسٹرکچر اور انٹیگریشن سروسز سےآگاہ ہونا چاہیے۔ ان موجودہ نفاذات کو دوبارہ استعمال کرنے سے سسٹم کو لاگو کرنے کے لیے درکار کام کم ہو جاتا ہے، جس‌سے بلڈ ٹیم بنیادی نظام کی فعالیت پر توجہ مرکوز کر سکتی ہے۔ دوبارہ استعمال پورے انٹرپرائز میں سسٹمز کے ساتھ‌تعامل میں منتظمین اور محافظوں کے لیے زیادہ مستقل مزاجی فراہم کرتا ہے۔

4.2.1مرئیت کے لیے عمارت

ڈیولپرزاور انجینئرز اپنے سسٹم کی مرئیت کو بہتر بنانے کے لیے جو سب سے موثر اقدام کرتے ہیں وہ مضبوط ایپلیکیشن‌لاگنگ کو نافذ کرنا ہے۔ ایپلیکیشن لاگز ایپلیکیشن کے مشن اور ایپلیکیشن کی سیکیورٹی سے متعلق دونوں واقعات‌کو ریکارڈ کرتے ہیں۔ بھرپور سیکورٹی لاگز روایتی اجازت/انکار اور کامیابی/ناکامی کے واقعات سے آگے بصیرت فراہم‌کرتے ہیں، یہ دکھانے کے لیے کہ ایپلیکیشن نے مختلف ان پٹ اور شرائط پر کیا رد عمل ظاہر کیا۔

مثال‌کے طور پر، یوزر ان پٹ جو کہ SQL اسٹیٹمنٹ کے پیرامیٹرز ہیں لاگ ان کیے جائیں اور اس کے نتیجے میں ایپلی کیشن ایکشن ریکارڈکیا جائے۔ اس کا استعمال کرتے ہوئے، ایک محافظ کو بصیرت حاصل ہوتی ہے کہ کون سا ایس کیو ایل انجیکشن ایپلی کیشن کوکامیابی کے ساتھ بلاک کرنے کی کوشش کرتا ہے اور کن کو بلاک کرنے میں ناکام رہا۔ مزید برآں، ایونٹ لاگز کے مواد سسٹم کی سرگرمی‌کو سافٹ ویئر اسٹیک میں اور وقت کے ساتھ دوبارہ تشکیل دینے کی اجازت دیتے ہیں۔ اس کا مطلب یہ ہے کہ ایونٹ کی IDs، صارف IDs، اور واقعات کو باہم مربوط کرنے کے لیے ضروری ٹائم سٹیمپ جیسی صفات شامل ہیں۔ محافظ اس تعمیر نو کو مؤثرطریقے سے انجام دینے کے لیے ضروری لاگ مواد پر ڈویلپرز کو رہنمائی فراہم کرتے ہیں۔

4.2.2انتظام کے لیے عمارت

ڈیفنڈایبل آرکیٹیکچر میں انتظامی خصوصیات کو نافذ کرنے کے لیے، ڈویلپرز انتظامیہ کے تمام افعال کو واضح طور پر بیان‌اور الگ کرتے ہیں۔ ایڈمنسٹریشن ٹریفک کو معیاری صارف کے ٹریفک سے فرق کرنے سے محافظوں کو زیادہ آسانی سےحملوں کی شناخت کرنے اور استحقاق کی کوششوں کو بلند کرنے کی اجازت ملتی ہے۔ یہ انتظامی انٹرفیس پر مضبوط‌کنٹرول کو بھی قابل بناتا ہے، جیسے کہ دو عنصر کی توثیق اور قابل اعتماد نیٹ ورک راستوں تک رسائی کو محدود‌کرنا۔

سسٹم‌کا دفاع کرنے کے لیے صرف پروڈکشن سرورز کی حفاظت سے زیادہ کی ضرورت ہوتی ہے۔ سورس کوڈ، مرتب کردہ ایگزیکیوٹیبل،کنفیگریشن فائلز، اور آپریٹنگ سسٹم کی تصاویر مجموعی طور پر سسٹم کے تمام حصے ہیں۔ ایک مخالف جو سسٹم کےسورس کوڈ میں بدنیتی پر مبنی سافٹ ویئر کو سرایت کرنے کے قابل ہوتا ہے وہ اس حد تک استثنیٰ کے ساتھ کام کرنے کے قابل ہوتاہے جس کا زیادہ تر سسٹم ڈیزائنرز کو اندازہ نہیں ہوتا ہے۔

لہذا،قابل دفاع فن تعمیر کے اصولوں کا اطلاق سورس کوڈ کنٹرول اجزاء، سسٹم کی تعمیر کے اسکرپٹس، اور ترقی اور جانچ‌کے ماحول پر کیا جاتا ہے۔ کوڈ، کنفیگریشن، اور ڈیٹا کو پیداواری ماحول میں منتقل کرنے کے طریقہ کار پر بھی گہری‌توجہ دی جاتی ہے۔ نظم و نسق کی اس شکل کو پیداواری ماحول میں تعینات تمام اجزاء کی فراہمی اور توثیق کےلیے درکار اقدامات کا حساب دینا چاہیے۔

4.2.3بقا کے لیے عمارت

کسی‌نظام میں بقا کی تعمیر اس کے ضروری ڈیٹا، افعال اور خدمات کی شناخت کے ساتھ شروع ہوتی ہے، جسے عام طورپر سسٹم کے خطرے کے تجزیہ کے حصے کے طور پر شناخت کیا جاتا ہے۔ اس کی بنیاد پر، ایک ترقیاتی ٹیم مناسب نفاذکے نمونوں اور اصولوں کا اطلاق کرتی ہے جیسے کہ فالتو پن، انکیپسولیشن، اور ڈیکپلنگ

اس‌بات کو یقینی بنائیں کہ جب انفرادی اجزاء ناکام ہو جائیں تو نظام کام کر سکتا ہے۔ ایک ایسا نظام تیار کرنا جو کلیدی اجزاء کے دستیاب‌نہ ہونے کی صورت میں خدمات کی شاندار تنزلی فراہم کرتا ہے آپریٹرز کو نظام کا استعمال جاری رکھنے کی اجازت دیتا ہے، یہاں‌تک کہ مداخلت کے تجزیہ اور بحالی کے دوران بھی۔

ڈویلپرزپس منظر کی نقل و حرکت کے مواقع کے لیے اندرونی اعتماد کی حدود کی بھی جانچ پڑتال کرتے ہیں۔ کچھ انٹرفیس میں حصہ لینے والےاجزاء کو ایک دوسرے پر مکمل اعتماد کرنے کی ضرورت ہوتی ہے۔ اس کے بجائے، ڈویلپرز کی وضاحت کرتے ہیں‌مقصداعتماد کا، اور اس‌مقصد کے لیے انٹرفیس کو محدود کریں۔ مثال کے طور پر، ڈیٹا بیس سرور کی بجائے کسی ویب سرور پر وسیع پیمانے پر بھروسہ کیا جاتاہے، DBMS کسی مخصوص ڈیٹا بیس مثال میں مخصوص جدولوں سے استفسار کرنے کے لیے ویب سرور کے سروس اکاؤنٹ پر بھروسہ‌کرتا ہے۔

ٹیسٹنگ‌سسٹم کی بقا میں بہت زیادہ حصہ ڈالتی ہے۔ شاید قابل دفاع آرکیٹیکچرز کی دیگر خصوصیات میں سے کسی‌سے زیادہ۔ جیسا کہ زیادہ تر سسٹمز کی دستیابی کے تقاضوں کے ساتھ، ٹیسٹرز سسٹم کی ناکامی یا جزو کی ناکامی‌کی صورت میں قابل قبول فعالیت فراہم کرنے کی صلاحیت کی تصدیق کرتے ہیں۔ اس کے علاوہ، ٹیسٹرز اس بات‌کی بھی تصدیق کرتے ہیں کہ نظام آن لائن ہونے کے دوران محافظ ضروری مداخلت کا تجزیہ کر سکتے ہیں۔ مثالوں میں‌فرانزک سسٹم کی تصاویر جمع کرنا، فائلیں اور بیک اپ بازیافت کرنا، اور تفصیلی سسٹم لاگز کو بازیافت کرنا شامل‌ہیں۔ جانچ بھی بغیر کسی رکاوٹ کے اجزاء کو واپس آن لائن رکھنے کی صلاحیت کی تصدیق کرتی ہے۔

یہ‌سمجھنے کے لیے جانچ ضروری ہے کہ کوئی نظام حملے میں کیسے کارکردگی کا مظاہرہ کرتا ہے۔ مجموعی طور پر ڈیفنڈ ایبل آرکیٹیکچرزکی طرح، ٹیسٹ ڈیزائن کو بھی دستیاب خطرے کی ذہانت کا فائدہ اٹھانا چاہیے۔ آزمائشی منصوبے جو کہ نظام کو نشانہ‌بنانے والے حملوں کی قسموں کی تقلید کرتے ہیں، سسٹم کے خطرے کے تجزیے اور TTPs اور مخالف مقاصد کے بارے میں خطرے‌کی انٹیلی جنس کے امتزاج کا استعمال کرتے ہوئے بنائے گئے ہیں۔ یہ ٹیسٹ منظرنامے نظام کے اندر ابتدائی حملے کی کوششوں‌اور پس منظر کی نقل و حرکت دونوں کو حل کرتے ہیں۔ اس کا مقصد یہ ہے کہ نظام کے فعال ہونے کی صلاحیت کو جانچناہے۔*دفاع کیا*. اس کے لیے جانچ کی ضرورت ہے نہ کہ نظام کتنا سخت ہے۔ لیکن یہ بھی کہ یہ کتنی اچھی طرح سے مرئیت، بقا، اورنظم و نسق فراہم کرتا ہے۔ جیسا کہ [1] میں بیان کیا گیا ہے، جانچ یہ ثابت نہیں کر سکتی کہ سسٹم محفوظ ہے۔ لیکن یہ تصدیق‌کر سکتا ہے کہ کنٹرول اس کا فعال طور پر دفاع کرتے ہیں۔

4.3قابل دفاع نظام چلانا

آپریٹرزاور منتظمین آپریشن کے دوران نظام کی سالمیت کو برقرار رکھنے کے ذمہ دار ہیں۔ ان کے پاس سسٹم کے ساتھ سب‌سے پہلے ہاتھ کا تجربہ بھی ہے، اور اس وجہ سے وہ تحقیقات اور تجزیہ میں محافظوں کی مدد کرنے کے لیے بہترین‌پوزیشن میں ہیں۔ ابتدائی پتہ لگانے کے انتباہات کو عام طور پر کسی سمجھوتے کی تصدیق کرنے سے پہلے مزید تجزیہ‌کی ضرورت ہوتی ہے۔ نظام کے بارے میں منتظمین کا علم محافظوں کو نظام کے اندر کی ترتیب اور "نارمل" سرگرمی‌کو بہتر طور پر سمجھنے میں مدد کرتا ہے، تاکہ یہ تعین کیا جا سکے کہ کن اجزاء سے سمجھوتہ کیا جا سکتا ہے۔اس لحاظ سے، نظاموں کی انوینٹری، ان کے ڈیزائن، اور ترتیب مرئیت کی ایک شکل ہے، جو ممکنہ طور پر سمجھوتہ‌کرنے والے نظام کا فوری تجزیہ کرنے کے لیے ضروری ہے۔

منتظمین‌پر سسٹم کے اندر خطرے کے انتظام کا بھی الزام عائد کیا جاتا ہے۔ ڈیزائن اور نفاذ کی بنیاد پر، ان میں سے کچھ‌سرگرمیاں، جیسے کہ پیچنگ، خودکار ہو سکتی ہیں۔ تاہم، زیادہ تر سسٹمز میں، سافٹ ویئر کے ذیلی سیٹ کو دستی‌طور پر منظم کرنے کی ضرورت ہوگی۔ اس کے لیے منتظمین کو سافٹ ویئر اپ ڈیٹس اور پیچ بروقت انجام دینے کی‌ضرورت ہے۔ اس کے لیے ان کے‌پاس سسٹم میں لائے جانے والے تمام ایگزیکیوٹیبلز کی صداقت کی تصدیق کرنے کے لیے‌عمل کی ضرورت ہوتی ہے۔ کوڈ پر دستخط کرنا ایک عام تکنیک ہے۔ تاہم جہاں ڈیلیور شدہ کوڈ پر دستخط نہیں کیے گئے‌ہیں وہاں مزید دستی عمل ضروری ہوسکتے ہیں۔ ایگزیکیوٹیبلز کی توثیق کرنے کی ضرورت تجارتی، اوپن سورس، اورکسٹم سافٹ ویئر پر یکساں طور پر لاگو ہوتی ہے۔ سبھی نظام کے خلاف ممکنہ حملہ کرنے والے ویکٹر کی نمائندگی کرتے‌ہیں، حالانکہ تخفیف ان کے درمیان مختلف ہو سکتی ہے۔

آخرمیں، ڈیفنڈ ایبل آرکیٹیکچرز پر مبنی سسٹمز کے ایڈمنسٹریٹرز کو سسٹم میں ڈیزائن کیے گئے انتظامی راستوں پر عمل‌کرنا چاہیے۔ نیٹ ورک کے ان راستوں، سافٹ ویئر انٹرفیسز، یا تصدیق کے طریقہ کار سے انحراف، ممکنہ طور پر محافظوں‌کے ذریعے غلط مثبت پتہ لگانے کو متحرک کرے گا۔

4.4قابل دفاع نظاموں کا دفاع کرنا

یہ‌مقالہ اس بات کی وضاحت کرنے کی کوشش نہیں کرتا ہے کہ انٹیلی جنس پر مبنی دفاعی تجزیہ کیسے کیا جائے، کیونکہ کئی متن‌اور پورا نصاب پہلے سے ہی دفاعی نظام کے طریقوں کی وضاحت کرتا ہے۔ اس کے بجائے، یہ سیکشن بیان کرتا ہے کہ کیسے

محافظدفاعی آرکیٹیکچرز کے ڈیزائن، ترقی، اور آپریشنز کی حمایت کر سکتے ہیں۔ یہ ان طریقوں کی بھی وضاحت کرتا ہےجن سے ان نظاموں کا زیادہ مؤثر طریقے سے دفاع کیا جاتا ہے۔

دفاعینظاموں میں عملی ڈیزائن پیش کیے جاتے ہیں جو مخالفین کے کام کرنے والے علم اور آپریشن کے دوران نظاموں کافعال طور پر دفاع کرنے کی ضرورت کے ذریعے کارفرما ہوتے ہیں۔ ڈیفنڈ ایبل آرکیٹیکچر میں محافظوں کی سب سے اہمشراکت خطرے کی ذہانت ہے۔ سائبر انٹیلی جنس کے تجزیے سے حاصل کردہ اپنے علم کو بانٹتے ہوئے، محافظ تنظیموںکو سیکیورٹی کنٹرولز کے انتخاب اور ان پر عمل درآمد کرنے میں عملی انتخاب کرنے میں مدد کرتے ہیں۔ یہ انتخابٹیموں کو سب سے زیادہ مؤثر کنٹرول کو اچھی طرح سے نافذ کرنے پر اپنی کوششوں پر توجہ مرکوز کرنے کی اجازتدیتے ہیں۔ مضبوط انٹیلی جنس مینجمنٹ کے عمل محافظوں کو TTPs اور مخالف مقاصد کے بارے میں معلوماتکو ڈیزائنرز اور ڈویلپرز کے ساتھ شیئر کرنے کی اجازت دیتے ہیں۔ مزید اہم بات یہ ہے کہ اعلیٰ درجے کی انٹیلی جنستجزیہ کی صلاحیتوں والی تنظیمیں TTPs، مخالف مقاصد، اور نئے مخالفین کے وجود میں رجحانات اور تبدیلیوںکو پہچاننے کے قابل ہیں۔ ان میں اہم تبدیلیاں قابلِ دفاع آرکیٹیکچرز کے بنیادی ڈھانچے اور ڈیزائن کے فیصلوں میںتبدیلیاں لاتی ہیں۔

محافظاپنی مرئیت کی ضروریات کو مواد اور مقام دونوں میں بتاتے ہیں۔ ایپلیکیشن لاگز کے بنیادی مواد کی وضاحت کر کے،مثال کے طور پر، محافظ مداخلت کی کوششوں کا تجزیہ کرنے کے لیے تاریخی نوشتہ جات میں آسانی سے محور بن سکتےہیں۔ یہ نیٹ ورک، OS، پلیٹ فارم، اور ایپلیکیشن سمیت پورے سسٹم اسٹیک میں متعلقہ سرگرمی کو بھی سپورٹکرتا ہے۔

اسزیادہ مرئیت کا استعمال کرتے ہوئے، محافظ کسی نظام کو سپورٹ کرنے والے حفاظتی کنٹرولز کے عین مطابق اصولوں کو جانچنے اور تعینات‌کرنے کے لیے اشارے استعمال کرنے کے قابل ہوتے ہیں۔ تاریخی ڈیٹا محافظوں کو نئے حملوں اور ماضی کی سرگرمیوں کے درمیان تعلقات‌تلاش کرنے کی اجازت دیتا ہے، جو مخالفین اور مہمات میں تبدیلیوں کے بارے میں نئی انٹیلی جنس کو ظاہر کرتا ہے۔ محافظ اس تاریخی‌ڈیٹا کے خلاف نئے سراغ لگانے اور مسدود کرنے کے قواعد کی جانچ بھی کرتے ہیں، جو قواعد کی درستگی پر اعتماد فراہم کرتے ہیں۔

ڈیفنڈایبل آرکیٹیکچرز کی انتظامی صلاحیت محافظوں کو ان نئے قواعد کو مناسب کنٹرولز میں تیزی سے اور درست طریقے سے تعینات‌کرنے کی اجازت دیتی ہے۔ زیادہ تر سسٹمز اور انٹرپرائزز میں اوور لیپنگ صلاحیتوں کے ساتھ سیکیورٹی کنٹرولز کا ایک وسیع‌سیٹ ہوتا ہے۔ قابل دفاع آرکیٹیکچرز نئے قوانین کی تعیناتی کے لیے سب سے مؤثر جگہ کی وضاحت فراہم کرنے میں مدد کرتے ہیں۔ان فیصلوں کو مرئیت کے پوائنٹس کے ساتھ کنٹرولز کی سیدھ اور محافظوں کی بصیرت سے آگاہ کیا جاتا ہے جس میں مرئیت‌کے ذرائع مطلوبہ اشارے کے ساتھ سب سے زیادہ قریب سے ہم آہنگ ہوتے ہیں۔

بلاشبہ،محافظوں کا سب سے قابل شناخت کردار دخل اندازی کا پتہ لگانا اور جواب دینا ہے۔ ڈیفنڈ ایبل آرکیٹیکچرز دفاع‌کرنے والوں کو سسٹم میں گہری فرانزک مرئیت دے کر مداخلت کے تجزیہ اور ردعمل کو بہتر بناتے ہیں۔ یہ سسٹمزکے آن لائن تجزیہ کو قابل بناتا ہے اور آف لائن فرانزک تجزیہ کے لیے ٹائم لائن کو مختصر کرتا ہے۔ مثال کے طور پر،ایجنٹ سافٹ ویئر انسٹال کرنے اور فزیکل میڈیا بھیجنے کے بجائے، نیٹ ورک پر فورینزک امیج کو فوری طور پر کیپچرکرنے اور منتقل کرنے کے قابل ہونا، اس عمل میں گھنٹے یا دن لگتے ہیں۔ مزید برآں، زندہ رہنے کے لیے بنائے گئے نظام‌مداخلت پر مشتمل ہوتے ہوئے تجزیہ اور بازیابی کے ذریعے اپنی خدمات کی فراہمی جاری رکھنے کے قابل ہیں، اس طرح‌صارف کے کاموں کو ختم کرنے میں کاروباری اثرات اور رکاوٹ کو کم سے کم کرتے ہیں۔

5قابل دفاع انٹرپرائز

انفرادی‌نظام اپنے طور پر محفوظ نہیں ہو سکتے۔ انٹیلی جنس پر مبنی دفاعی حل سب سے زیادہ موثر ہوتے ہیں جب ایک‌پوری تنظیم میں کارکردگی کا مظاہرہ کیا جاتا ہے، اور کسی صنعت کے اندر انٹیلی جنس شیئرنگ سے بھرپور ہوتا ہے۔اسی طرح، قابل دفاع آرکیٹیکچرز بڑے پیمانے پر اپنے ماحول اور انٹرپرائز کے تناظر میں موجود ہیں۔ بہت سے مرئیت،انتظامی قابلیت، اور بقا کے کنٹرولز جو دفاعی آرکیٹیکچرز کو روایتی معلوماتی تحفظ کے طریقوں سے ممتاز کرتےہیں ایک قابل دفاع انٹرپرائز پر لاگو کیے جا سکتے ہیں۔ ایک قابل دفاع انٹرپرائز کا بنیادی ڈھانچہ بیک وقت مرئیت کےدورانیے کو بڑھاتا ہے جو محافظوں کے اختیار میں ہوتا ہے، اور ماحول میں لگائے گئے نظاموں کی لاگت اور پیچیدگی کوکم کرتا ہے۔

جیساکہ انفرادی نظام کی تعمیر کے ساتھ، ایک قابل دفاع انٹرپرائز کا انتظام خطرے کے تجزیے اور خطرے کی ذہانت سےشروع ہوتا ہے۔ تھریٹ ماڈلنگ اور تجزیہ کو انٹرپرائزز کے مطابق ڈھال لیا جا سکتا ہے۔

اسی‌طرح جیسے انفرادی نظاموں پر لاگو کیا جا سکتا ہے۔ درج ذیل جدول دکھاتا ہے کہ IDDIL/ATC طریقہ کار کو [6] سےانٹرپرائز تجزیہ تک کیسے لاگو کیا جائے۔

خطرےکے تجزیہ کا مرحلہ	انٹرپرائزتجزیہ قدم
میںاثاثوں کی نشاندہی کریں۔	بڑےانٹرپرائز اثاثوں کی شناخت کریں (مثال کے طور پر، ERP) اور اثاثوں کی کلاسیں (مثال کے طور پر، ویب سرورز)
ڈیحملے کی سطح efine	انٹرپرائزکی حدود کی وضاحت کریں (مثال کے طور پر، انٹرنیٹ گیٹ ویز، میل گیٹ ویز، آف سائٹ بیک‌اپ، آف نیٹ ورک ورک سٹیشن)
ڈیecompose	رسک‌اور پیچیدگی کی بنیاد پر انٹرپرائز کے پہلوؤں کو گلنا
میںحملے کے ویکٹر کی شناخت کریں۔	موجودہ‌اور ابھرتے ہوئے اٹیک ویکٹر کو واضح کرنے کے لیے خطرے کی ذہانت کا استعمال کریں۔ دماغی‌طوفان غیر استعمال شدہ یا غیر دریافت شدہ حملہ ویکٹر۔
ایلیہ دھمکی دینے والے اداکار ہیں۔	خطرےکے اداکاروں کی معلوم کلاسوں اور ان کے مقاصد کو واضح کرنے کے لیے خطرے کی ذہانت کا استعمال کریں۔غیر دریافت شدہ یا مستقبل کے خطرے والے اداکاروں کو ذہن میں رکھیں۔
اےتجزیہ اور تشخیص‌کے	شناخت‌شدہ خطرات کی بنیاد پر ممکنہ کاروباری اور تکنیکی اثرات کا تعین کریں۔
ٹیریج	اثرات،خطرے کی انٹیلی جنس، اور دستیاب تخفیف کی بنیاد پر خطرات اور تخفیف‌کو ترجیح دیں
سیکنٹرولز	نیاتعینات کریں اور موجودہ کنٹرول انفراسٹرکچر کو اپ ڈیٹ کریں۔

تصویر12:انٹرپرائز کی سطح پر خطرے کا تجزیہ

یہ‌تجزیہ سیکیورٹی کے بنیادی ڈھانچے کی سرمایہ کاری کو ایک معروضی انداز میں خطرات کی بنیاد پر ترجیح دینے کی‌اجازت دیتا ہے۔ حملے کی اقسام میں نئے رجحانات نئی قسم کی بنیادی ڈھانچے کی خدمات کی ضرورت پیدا کر سکتےہیں۔ یہ انٹرپرائزز کو فرسودہ قدر کی بنیاد پر موجودہ سیکیورٹی سروسز کو کم کرنے یا ریٹائر کرنے کی بھی اجازت دیتاہے۔ کچھ حفاظتی فعالیت جو ابتدائی تعیناتی کے وقت انتہائی موثر (اور مہنگی) تھی اجناس کی حیثیت میں واپس‌آ جاتی ہے۔ وہ خدمات جو اجناس کی سطح کے حفاظتی کنٹرول فراہم کرتی ہیں ان کو تنظیم کے بجٹ کا کموڈٹی سطح‌کا حصہ دینا چاہیے۔ تھریٹ انٹیلی جنس انفراسٹرکچر کی تعیناتی کے وقت سے بھی آگاہ کرتی ہے۔ مثال کے طور پر،بعض مخالفوں کی سرگرمیوں کی چکراتی نوعیت کو بنیادی ڈھانچے کے نفاذ کے وقت کو ترجیح دینے کے لیے استعمال‌کیا جا سکتا ہے۔

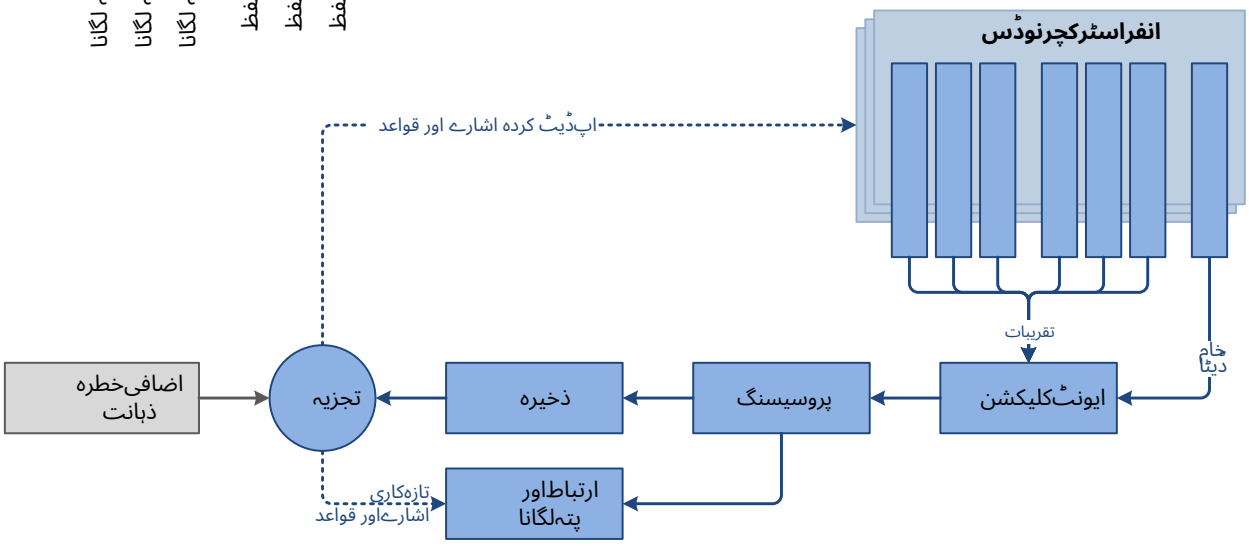
جس‌طرح سسٹم کے مجموعی فن تعمیر کو سسٹم کے سیاق و سباق کا حساب دینا چاہیے، اسی طرح سسٹم کے سیکیورٹی‌کنٹرولز کو بھی انٹرپرائز کے دفاعی انفراسٹرکچر کا حساب دینا چاہیے۔ دستیاب انفراسٹرکچر کا استعمال پورےسسٹمز میں کنٹرولز کے مستقل نفاذ کو یقینی بناتا ہے، اور محافظوں کو پورے انٹرپرائز میں جامع مرئیت اور انتظام‌کی اہلیت فراہم کرتا ہے۔ اہم بات یہ ہے کہ عام انفراسٹرکچر سسٹم کی ایک بڑی تعداد کو فوری طور پر نئے اشارے اوراس کے نتیجے میں ہونے والے قواعد سے فائدہ اٹھانے کی اجازت دیتا ہے کیونکہ وہ بنیادی ڈھانچے کے کنٹرول میں تعیناتہوتے ہیں۔ سب سے موثر ڈیفنڈ ایبل انٹرپرائزز نئے انکشاف کردہ اشاریوں کو چند مراحل میں اپ ڈیٹ کنٹرولز میں‌ترجمہ کر سکتے ہیں۔ یہ تدبیری تخفیف کے لیے خاص طور پر اہم ہے، جیسے کہ 2014 میں Heartbleed اور Shellshock جیسی وسیع پیمانے پر کمزوریوں کے انکشاف کے معاملے میں۔

ڈیفنڈایبل انٹرپرائز انفراسٹرکچر کی قدر بڑی حد تک بنیادی ڈھانچے کا فائدہ اٹھانے والے انٹرپرائز وسیع سسٹمز کے ذریعہ‌فراہم کردہ مرئیت کی بھرپور شکلوں سے ہوتی ہے۔ ایک قابل دفاع انٹرپرائز اس بات کو یقینی بناتا ہے کہ ڈیزائنرز، ڈویلپرز،اور منتظمین دستیاب بنیادی ڈھانچے اور خدمات، ان کی فعالیت، انٹرفیس، اور ان سے بہترین فائدہ اٹھانے کےلیے سسٹمز کو پوزیشن دینے کے طریقہ کو سمجھتے ہیں۔ مثال کے طور پر، اگر NIDS ڈکرپٹ شدہ شکل میں تمام ٹریفک‌کا معائنہ کرنے کے قابل ہو تو نیٹ ورک انٹروژن ڈٹیکشن سسٹم سے سسٹم کو فائدہ ہوتا ہے۔ کئی ڈیزائن متبادل اس‌مقصد کو حاصل کر سکتے ہیں؛ ڈیزائنرز اور ڈویلپرز کو اپنے سسٹم کے لیے انتخاب اور تجارت کو سمجھنا چاہیے۔ سیکورٹی‌کے بنیادی ڈھانچے اور خدمات کا ایک کیٹلاگ

انکی یکساں تفہیم کو فروغ دینے اور انٹرپرائز میں تمام سسٹمز کے استعمال میں مدد کرتا ہے۔ فنکشنل کنٹرول کا درجہ بندی [6] میںایسے ہی ایک کیٹلاگ کا خاکہ پیش کرتا ہے۔

ڈیزائنرز،ڈویلپرز، اور منتظمین کے ذریعے استعمال ہونے والی حفاظتی خدمات کا ایک ہی کیٹلاگ بھی محافظوں کے ذریعے اس‌بات کا اندازہ لگانے کے لیے استعمال کیا جاتا ہے کہ کن اشارے کے لیے کون سے قسم کے کنٹرول بہترین ہیں۔ ڈیزائن، تعمیر،چلانے اور دفاع کے مراحل کے درمیان اس مستقل مزاجی کا اضافی فائدہ ہے کہ وہ مخالف کارروائیوں کے خلاف سیکیورٹی‌کنٹرولز کی افادیت کو ٹریک کرنے کے قابل ہے۔ دفاع کرنے والے تجزیہ کرتے ہیں کہ ہر مخالف مہم کے لیے کون سے کنٹرولزکا پتہ چلا یا روکا گیا دخل اندازی کی کوششیں، مخالف سرگرمیوں کے بارے میں بصیرت، ان کے خلاف کنٹرول کی تاثیر،اور گمشدہ کنٹرولز، جس سے کاروباری اداروں کو اپنے حفاظتی کنٹرولز کی قدر کا اندازہ لگانے اور مستقبل میں بہتری کی‌منصوبہ بندی کرنے کی اجازت ملتی ہے۔ نتیجے کے طور پر، انٹرپرائز کی سطح پر انتظامی صلاحیت کو نئے قواعد کی تعیناتی‌کے لیے رفتار اور درستگی دونوں میں اور محافظ کی ان اصولوں کی افادیت کا اندازہ لگانے کی صلاحیت میں ماپا جاتاہے۔

مرئیت‌کی وسعت قابل دفاع انٹرپرائز کی بنیاد ہے۔ نیٹ ورک اور سسٹم کی سرگرمی کو جمع کرنا اور برقرار رکھنا پتہ لگانے‌کے کنٹرول کو ترجیح دینے کے لیے ضروری بصیرت فراہم کرتا ہے اور کاروباری معاملات کو شناخت سے بلاک کرنے کی‌طرف منتقل کرنے کے لیے تیار کرتا ہے۔ یہ منتقلی لائیو ڈیٹا اور تاریخی ڈیٹا کے خلاف تشخیص کے ساتھ عملی تجربے کی‌بنیاد پر پتہ لگانے اور بلاک کرنے کے قوانین کی وفاداری کے ذریعے قابل اعتماد ہے۔ ایک لچکدار فن تعمیر جو جمع کرنےاور پتہ لگانے کے سلسلے کے اوپر فعال بلاکنگ کنٹرول بناتا ہے، جیسا کہ شکل 13 میں دکھایا گیا ہے، قابل دفاع انٹرپرائزکو اپنے بنیادی ڈھانچے میں اضافی سرمایہ کاری کرنے دیتا ہے۔ قاعدے کی پیچیدگی اور تقسیم شدہ سینسر کی‌صلاحیت پر منحصر ہے، پتہ لگانے کے قواعد کو ان لائن یا مرکزی طور پر تعینات کیا جا سکتا ہے۔ ایک ہی پائپ لائن میں‌بلاکنگ اور پتہ لگانے کے قوانین کو سیدھ میں لانا بھی انٹرپرائز کو اس قابل بناتا ہے کہ وہ موجودہ پائپ لائنوں پر نئےپتہ لگانے اور بلاک کرنے والے ماڈیولز کی تعیناتی کے ذریعے مخالف TTPs میں ہونے والی تبدیلیوں کو آسانی سے ڈھال‌سکے۔



تصویر13:انٹرپرائز کی مرئیت اور نظم و نسق کے لیے مشترکہ مجموعہ، کھوج، اور بلاکنگ انفراسٹرکچر

انٹرپرائزکی بقاء مجموعی طور پر انٹرپرائز پر ایک جیسے سسٹم کی سطح کے بہت سے اصولوں کا اطلاق کرتی ہے۔ ہم آہنگی،جوڑے، اور سیگمنٹیشن ڈیزائن کے ضروری تحفظات ہیں، کیونکہ پس منظر کی حرکت ایک حد تک مشترکہ خطرےکو متعارف کراتی ہے جس کا انفرادی نظام ڈیزائنرز آسانی سے حساب نہیں رکھتے۔ تنظیم میں تبدیلیوں، انضمام،حصول اور تقسیم کے دوران اثرات کو کم کرنے کے لیے، پورے انٹرپرائز میں تقسیم کاروباری ڈھانچے کے انتہائی مستحکم‌پہلوؤں کے ساتھ منسلک ہے۔ سیگمنٹیشن پورے اسٹیک میں ٹیکنالوجی کا بھی فائدہ اٹھاتا ہے، بشمول نیٹ ورک،ورچوئلائزیشن، آپریٹنگ سسٹم، شناخت اور رسائی کا انتظام، اور ایپلیکیشن کی فعالیت۔

کسیانٹرپرائز کی مجموعی سلامتی کا انحصار حملوں کے خلاف اس کی لچک پر اور حملہ آوروں میں ہونے والی تبدیلیوںکے لیے اس کی لچک پر بھی ہے۔ ان دونوں میں کسی تنظیم کو مغلوب کرنے کی صلاحیت ہے، چاہے انفرادی حملوںکا جواب دینا ہو، یا مخالفین اور ان کے مقاصد میں تبدیلیوں سے نمٹنے کے لیے انفراسٹرکچر میں سرمایہ کاری کرنا۔ڈیفنڈ ایبل انٹرپرائز اپنی خطرے کی ذہانت اور انٹرپرائز کے خطرے کے تجزیے سے فائدہ اٹھاتا ہے تاکہ لچکدار سیکیورٹیانفراسٹرکچر اور ایک زندہ رہنے کے قابل IT انفراسٹرکچر بنایا جا سکے۔ یہ تنظیموں کو اپنے نظام اور اثاثوں کے ڈیزائن،ترقی، آپریشنز اور دفاع میں موثر فیصلے کرنے کے قابل بناتا ہے۔

6خلاصہ

کلاسیکیسیکورٹی انجینئرنگ اور فن تعمیر غلط مسئلے کو حل کرنے کی کوشش کر رہا ہے۔ تعمیر کرنے کی کوشش کرنا کافی نہیںہے۔*سخت*نظام اس کے بجائے ہمیں ایسے نظاموں کی تعمیر کرنی چاہیے۔*قابل دفاع*. سسٹم کی ضروریات، ڈیزائن، یا ٹیسٹکے نتائج کو "محفوظ" قرار نہیں دیا جا سکتا۔ بلکہ، یہ اس بات کا مجموعہ ہے کہ سسٹم کو کس طرح ڈیزائن کیا گیا، بنایاگیا، چلایا گیا اور اس کا دفاع کیا گیا جو بالآخر وقت کے ساتھ ساتھ نظام اور اس کے اثاثوں کی حفاظت کرتا ہے۔ چونکہ مخالفینبدلتے ہوئے مقاصد اور مواقع کی بنیاد پر اپنی تکنیکوں کو اپناتے ہیں، اس لیے نظاموں اور کاروباری اداروں کا فعال طورپر دفاع کیا جانا چاہیے۔

قابلدفاع آرکیٹیکچرز ان نظاموں کی نمائندگی کرتے ہیں جو انٹیلی جنس پر مبنی دفاعی طریقوں کے لیے بنائے گئے ہیں۔ وہڈیزائنرز، ڈویلپرز، منتظمین، اور محافظوں کے علم کا فائدہ پورے نظام کے لائف سائیکل میں لیتے ہیں۔ اس طرح سے،تنظیمیں اپنے سسٹمز میں نافذ سیکیورٹی کنٹرولز کے بارے میں باخبر اور عملی فیصلے کرتی ہیں۔ ان کے فعال دفاعکو مؤثر طریقے سے سپورٹ کرنے کے لیے، ڈیفنڈ ایبل آرکیٹیکچرز پر بنائے گئے سسٹمز مرئیت، انتظام اور بقا کی خصوصیاتکا اظہار کرتے ہیں۔

توسیعکے ذریعے، ان تصورات کو ایک قابل دفاع انٹرپرائز بنانے کے لیے بڑے پیمانے پر لاگو کیا جاتا ہے۔ یہ تنظیمیں اپنے خطرےکے تجزیے اور خطرے کی انٹیلی جنس کو حفاظتی ڈھانچے کو ڈیزائن، تعینات کرنے اور چلانے کے لیے استعمال کرنےکے قابل ہیں جو ان کی دفاعی ضروریات کو پورا کرتا ہے۔ ایک ڈیفنڈ ایبل انٹرپرائز نئی خطرے کی ذہانت کو تازہ ترین دستخطوں، بنیادی ڈھانچے کی تبدیلیوں، اور سسٹم کے ڈیزائن کے نمونوں میں مؤثر طریقے سے ترجمہ کرنے کے قابل ہے، جس سے وہ اپنے مخالفین کو مؤثر طریقے سے جواب دینے کے قابل ہے۔ ایسی تنظیمیں انٹرپرائز کی سطح کے خطرےکی انٹیلی جنس اور خطرے کے تجزیہ کی بنیاد پر نئے سیکیورٹی انفراسٹرکچر کی تعیناتی کے بارے میں باخبر فیصلےکرنے کے قابل بھی ہیں۔

سائبرلچک حاصل کرنے کی کوشش کرنے والی تنظیموں کو حملوں سے بچنے کی ضرورت اور ایسے فن تعمیرات پر غور کرناچاہیے جو حملہ آور کی تکنیکوں اور مقاصد میں تبدیلیوں کے لیے لچکدار ہوں۔ خطرے کی ذہانت سے فائدہ اٹھاتے ہوئےاور مرئیت، نظم و نسق اور بقا کے لیے ڈیزائننگ کے ذریعے، تنظیموں اور ان کے نافذ کردہ نظاموں کا فعال طور پر دفاعکیا جاتا ہے اور نئی قسم کے حملوں کے مطابق ڈھال لیا جاتا ہے۔

حوالہجات

[1] محکمہ دفاع، دفاعی سائنس بورڈ، "لچکدار ملٹری سسٹمز اینڈ دی ایڈوانسڈ سائبر تھریٹ،" آفس آف دی انڈر سیکرٹریبرائے دفاع برائے حصول، ٹیکنالوجی، اور لاجسٹکس، واشنگٹن، ڈی سی، 2013۔

[2] ورلڈ اکنامک فورم؛ میک کینسی اینڈ کمپنی، "ہائپر کنیکٹڈ دنیا میں خطرہ اور ذمہ داری،" ورلڈ اکنامک فورم، جنیوا،2014۔

LR Young, "CERT Resilence Management Model, Version 1.0," Software Engineering Institute, 2010۔]3[RA Caralli, JH Allen, PD Curtis, DW White and

[4] "صدارتی پالیسی ہدایت نامہ / PPD-21 -- اہم انفراسٹرکچر سیکورٹی اور لچک"۔

Network Defence informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"
R. Amin، M. Cloppert اور E. Hutchins، "Intelligence-driven Computer [5] *انفارمیشن وارفیئر اور سیکیورٹی پر 6ویں بین الاقوامی کانفرنس کی کارروائی*، 2011۔

M. Muckin اور SC Fitch، "A Threat-driven Approach to Cyber Security," 2014۔ [6]

http://techblog.netflix.com/2012/07/chaos-monkey-released-into-wild.html: جولائی 2012۔ [آن لائن]۔
A. Tseitlin، "Chaos Monkey Released Into The Wild،" 30 دستیاب اور C. Bennett [7]