BACKGROUNDERS
Press Information Bureau
Government of India

سی ای آر ٹی اِن: سائبر خطرات کے خلاف بھارت کا اولین دفاعی قلعہ(فرنٹ لائن ڈیفنڈر)

ایک محفوظ، قابلِ اعتماد اور جوابدہ سائبر اسپیس کی تشکیل

کلیدی نکات

- 2025میں سی ای آر ٹی-اِن نے 29.44 لاکھ سے زائد سائبر واقعات سے مؤثر طور پر نمٹا، جس کے دوران 1,530 الرٹس، 390 کمزوریوں سے متعلق نوٹس اور 65 ایڈوائزریز جاری کی گئیں، جو قومی سطح پر سائبر ردِعمل کی مضبوط اور ہمہ گیر صلاحیت کی عکاسی کرتی ہیں۔
- 231سائبر سیکیورٹی آڈٹ تنظیموں کو پینل میں شامل کیا گیا، جس سے اہم انفارمیشن و کمیونیکیشن ٹیکنالوجی (آئی سی ٹی) بنیادی ڈھانچے میں آڈٹ اور کمزوریوں کی تشخیص کی صلاحیت کو نمایاں طور پر تقویت ملی۔
- سائبر سوچھتا کیندر کے ذریعے ملک کی 98 فیصد ڈیجیٹل آبادی کا احاطہ کیا گیا، 1,427 تنظیموں کو آن بورڈ کیا گیا، جبکہ 89.55 لاکھ میلویئر ہٹانے والے ٹولز ڈاؤن لوڈ کیے گئے۔
- سی ای آر ٹی-اِن کی مسلسل اور منظم سائبر سیکیورٹی کوششوں کو عالمی سطح پر تسلیم کیا گیا ہے، جہاں عالمی اقتصادی فورم، آکسفورڈ یونیورسٹی اور فرانس کی اے این ایس ایس آئی جیسے ممتاز بین الاقوامی اداروں نے اے آئی پر مبنی خطرات کی نشاندہی، سائبر لچک، قابلِ اعتماد اے آئی فریم ورک اور شہریوں پر مرکوز میلویئر تخفیف کے میدان میں ہندوستان کی قیادت کا اعتراف کیا ہے۔

تعارف

ہندوستان کی تیز رفتار ڈیجیٹل تبدیلی نے غیر معمولی پیمانے پر حکمرانی، تجارت اور شہری خدمات کے ڈھانچے کو نئی شکل دی ہے۔ ڈیجیٹل ادائیگیوں اور ای-کامرس

سے لے کر آن لائن عوامی خدمات کی فراہمی تک، ڈیجیٹل ٹیکنالوجی روزمرہ زندگی کا ایک لازمی جزو بن چکی ہے۔ جیسے جیسے ڈیجیٹل اپنانے کی رفتار میں اضافہ ہو رہا ہے، سائبر اسپیس کا تحفظ قومی ترجیح کے طور پر نمایاں ہو کر سامنے آیا ہے۔

آن لائن دھوکہ دہی، فِشنگ، رینسم ویئر حملوں، مصنوعی ذہانت سے چلنے والے گھوٹالوں اور اہم ڈیجیٹل بنیادی ڈھانچے کو درپیش بڑھتے ہوئے خطرات کے تناظر میں ایک مربوط، مضبوط اور لچکدار سائبر سیکیورٹی فریم ورک کی ضرورت پہلے سے کہیں زیادہ محسوس کی جا رہی ہے۔ ان چیلنجز کو مدنظر رکھتے ہوئے حکومتِ ہند نے ایک محفوظ، قابلِ اعتماد اور مستحکم ڈیجیٹل ماحول کے قیام کے لیے جامع پالیسیوں، مؤثر ادارہ جاتی نظام اور مضبوط عملی صلاحیتوں کو بروئے کار لایا ہے۔

ہندوستان کے سائبر سیکیورٹی ڈھانچے کے مرکز میں انڈین کمپیوٹر ایمرجنسی رسپانس ٹیم (سی ای آر ٹی-اِن) موجود ہے، جو وزارتِ الیکٹرانکس و اطلاعاتی ٹیکنالوجی (ایم ای آئی ٹی وائی) کے تحت کام کرتی ہے اور انفارمیشن ٹیکنالوجی ایکٹ، 2000 کے تحت باقاعدہ طور پر قائم کی گئی ہے۔ سی ای آر ٹی-اِن واقعات کے مؤثر انتظام، نظامی لچک میں اضافے اور حکومت، صنعت اور معاشرے میں محفوظ ڈیجیٹل طریقۂ کار کے فروغ کے ذریعے قومی سائبر دفاع کو ادارہ جاتی مضبوطی فراہم کرتی ہے۔ اس کا کردار ہندوستان کے تیزی سے وسعت اختیار کرتے ڈیجیٹل ماحولیاتی نظام کے تحفظ کو تقویت دیتا ہے اور ڈیجیٹل پلیٹ فارمز اور خدمات پر عوامی اعتماد کو مستحکم بناتا ہے۔

آج کے باہم مربوط ڈیجیٹل منظرنامے میں سائبر سیکیورٹی محض ایک تکنیکی معاملہ نہیں رہی، بلکہ قومی سلامتی، معاشی استحکام اور عوامی اعتماد کا ایک بنیادی ستون بن چکی ہے۔ ڈیجیٹل نظام کے بڑھتے ہوئے پیمانے اور پیچیدگی مسلسل چوکسی، مربوط کارروائی اور مضبوط ادارہ جاتی قیادت کے متقاضی ہیں۔ پالیسی رہنمائی کو عملی تیاری کے ساتھ ہم آہنگ کرتے ہوئے، سی ای آر ٹی-اِن نہ صرف ابھرتے ہوئے سائبر خطرات کا مؤثر جواب دیتا ہے بلکہ پیشگی اندازہ، لچک کی تعمیر اور اس امر کو یقینی بنانے میں بھی کلیدی کردار ادا کرتا ہے کہ ہندوستان کی ڈیجیٹل ترقی محفوظ، جامع اور پائیدار بنیادوں پر آگے بڑھے۔

ہندوستان کا بڑھتا ہوا ڈیجیٹل منظرنامہ

گزشتہ دہائی کے دوران ہندوستان کے ڈیجیٹل نقشِ قدم میں غیر معمولی تیزی سے اضافہ ہوا ہے، جس کی بنیادی وجوہات انٹرنیٹ کی بڑھتی ہوئی رسائی، اسمارٹ فونز کا وسیع پیمانے پر استعمال اور ڈیجیٹل عوامی خدمات کی برق رفتار توسیع ہیں۔ 2025 تک ہندوستان میں انٹرنیٹ کنکشنز کی تعداد 100 کروڑ کا سنگِ میل عبور کرتے ہوئے 100.29 کروڑ تک پہنچ گئی، جبکہ مارچ 2014 میں یہ تعداد محض

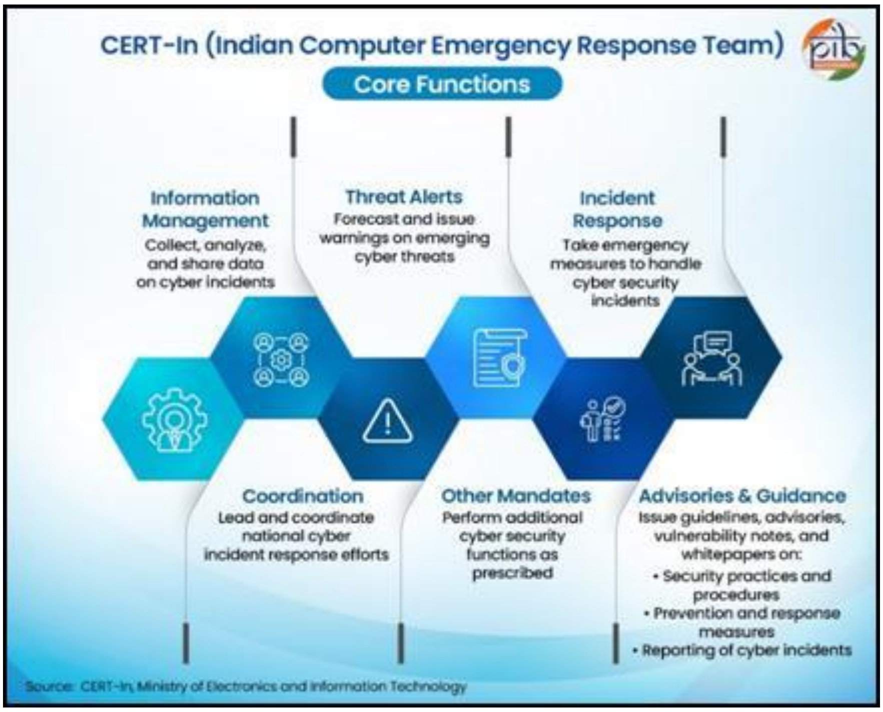
25.15 کروڑ تھی۔ فی وائرلیس ڈیٹا سبسکرائبر اوسط ماہانہ ڈیٹا استعمال میں تقریباً 399 گنا اضافہ ریکارڈ کیا گیا، جو 2014 میں 61.66 ایم بی سے بڑھ کر 2025 میں 24.01 جی بی تک پہنچ گیا، جو عالمی سطح پر سب سے زیادہ شمار ہوتا ہے۔

اس مضبوط ڈیجیٹل بنیاد نے ڈیجیٹل ادائیگیوں کے شعبے میں نمایاں ترقی کو ممکن بنایا ہے۔ یونیفائیڈ پیمنٹس انٹرفیس (یو پی آئی) ہندوستان کے ڈیجیٹل ادائیگی ایکو سسٹم کا مرکزی ستون بن کر ابھرا ہے۔ صرف دسمبر 2025 میں یو پی آئی کے ذریعے 21 ارب سے زائد لین دین انجام پائے، جن کی مجموعی مالیت 27 لاکھ کروڑ روپے سے بھی زیادہ تھی۔ اگرچہ اس ڈیجیٹل توسیع نے سہولت اور شمولیت میں خاطر خواہ اضافہ کیا ہے، تاہم اس کے ساتھ ساتھ سائبر خطرات کے لیے حملوں کی سطح بھی وسیع ہوئی ہے۔ ان چیلنجز سے نمٹنے کے لیے مرکزی بجٹ 2025-26 میں سائبر سیکیورٹی کے لیے 782 کروڑ روپے مختص کیے گئے، جو حکومت کی جانب سے ہندوستان کے ڈیجیٹل بنیادی ڈھانچے کے تحفظ پر مضبوط توجہ کی عکاسی کرتا ہے۔

اس پس منظر میں سی ای آر ٹی-اِن کا کردار ہندوستان کے سائبر سیکیورٹی فریم ورک کی بنیاد کے طور پر غیر معمولی اہمیت اختیار کر گیا ہے۔ سی ایس آئی آر ٹی-فِن، جو سی ای آر ٹی-اِن کے تحت مالیاتی شعبے کے لیے کمپیوٹر سیکیورٹی انسیڈنٹ رسپانس ٹیم کے طور پر کام کرتا ہے، مربوط واقعہ جاتی ردِعمل، معلومات کے تبادلے اور بینکنگ، مالیاتی خدمات اور انشورنس (بی ایف ایس آئی) شعبے کے لیے رہنمائی و معاونت فراہم کر کے مالیاتی نظام میں سائبر سیکیورٹی کو مستحکم بناتا ہے۔ اسی طرح سی ایس آئی آر ٹی-پاور، سی ای آر ٹی-اِن کے ایک توسیعی بازو کے طور پر کام کرتے ہوئے، سائبر واقعات کی نگرانی اور تجزیہ، سی ای آر ٹی-اِن کی فراہم کردہ سائبر خطرہ انٹیلی جنس پر عمل درآمد، صورتحال سے متعلق آگاہی کی بنیاد پر بروقت کنٹینمنٹ اقدامات، سائبر سیکیورٹی آڈٹس کو یقینی بنانے اور سی ای آر ٹی-اِن کے سائبر سوچھتا کیندر (سی ایس کے) کی رپورٹس کے مطابق خطرات میں کمی کے ذریعے پاور سیکٹر کی مجموعی سائبر سیکیورٹی پوزیشن کو مضبوط کرتا ہے۔

قومی سائبر سیکیورٹی کے لیے سی ای آر ٹی-اِن کے بنیادی فرائض

سی ای آر ٹی-اِن ہندوستان میں سائبر واقعات کے ردِعمل کے لیے قومی سطح کی مرکزی ایجنسی ہے۔ انفارمیشن ٹیکنالوجی ایکٹ، 2000 کی دفعہ 70 بی کے تحت اس کے مینڈیٹ میں سائبر حملوں کی روک تھام، سائبر خطرات کی حقیقی وقت میں نگرانی، اور سائبر واقعات کو کم کرنے اور ان پر قابو پانے کے لیے متعلقہ اسٹیک ہولڈرز کے ساتھ تیز اور مؤثر ہم آہنگی شامل ہے۔



CERT-In (Indian Computer Emergency Response Team)

Core Functions

Information Management
Collect, analyze, and share data on cyber incidents

Threat Alerts
Forecast and issue warnings on emerging cyber threats

Incident Response
Take emergency measures to handle cyber security incidents

Coordination
Lead and coordinate national cyber incident response efforts

Other Mandates
Perform additional cyber security functions as prescribed

Advisories & Guidance
Issue guidelines, advisories, vulnerability notes, and whitepapers on:
- Security practices and procedures
- Prevention and response measures
- Reporting of cyber incidents

Source: CERT-In, Ministry of Electronics and Information Technology

سی ای آر ٹی-اِن کے بنیادی افعال

سی ای آر ٹی-اِن کے بنیادی فرائض میں تنظیموں اور عام شہریوں کے مابین سائبر سیکیورٹی سے متعلق آگاہی کو فروغ دینا شامل ہے، تاکہ محفوظ ڈیجیٹل طرزِ عمل کو فروغ دیا جا سکے۔ یہ ادارہ اپنے خودکار سائبر تھریٹ ایکسچینج پلیٹ فارم کے ذریعے معلومات کے مؤثر تبادلے کو آسان بناتا ہے اور مختلف شعبوں سے وابستہ تنظیموں کے ساتھ موجودہ اور ممکنہ سائبر خطرات کے بارے میں قریب قریب حقیقی وقت کی معلومات کا اشتراک کرتا ہے۔ سی ای آر ٹی-اِن بین الاقوامی شراکت داروں، صنعت اور تعلیمی اداروں کے ساتھ قریبی تعاون کے ذریعے عالمی بہترین طریقۂ کار اور تجربات سے استفادہ کرتا ہے۔

اس کے ساتھ ساتھ، سی ای آر ٹی-اِن باقاعدگی سے تربیتی پروگراموں اور سائبر سیکیورٹی مشقوں کا انعقاد کرتا ہے تاکہ ادارہ جاتی تیاری کو مستحکم کیا جا سکے۔ سائبر حفظانِ صحت کو یقینی بنانے کے لیے سائبر سوچھتا کیندر (سی ایس کے) کا انتظام، سائبر خطرات اور حملہ آور مہمات کی نگرانی کے لیے کمانڈ اینڈ کنٹرول سینٹر کا قیام، اور اہم قومی و بین الاقوامی مواقع کے دوران تنظیموں اور اسٹیک ہولڈرز کے ساتھ تخفیفی اقدامات کی ہم آہنگی بھی اس کے کلیدی فرائض میں شامل ہیں۔ ادارہ ذمہ دارانہ کمزوری کے انکشاف کو ایک منظم ادارہ جاتی عمل کے طور پر فروغ دیتا ہے اور سائبر فارنزک صلاحیتوں کے ذریعے سائبر واقعات کی تفتیش میں قانون نافذ کرنے والے اداروں کی معاونت کرتا ہے۔ مزید برآں، قومی تیاریوں کو مضبوط بنانے کے لیے سائبر کرائسز مینجمنٹ پلان کے نفاذ میں تنظیموں کی رہنمائی اور انہیں فعال بنانا بھی سی ای آر ٹی-اِن کی ذمہ داریوں کا حصہ ہے۔

مسلسل آپریشنل مشغولیت اور مربوط ردِعمل کے نظام کے ذریعے، سی ای آر ٹی-اِن سائبر واقعات کی بروقت روک تھام کو یقینی بناتا ہے اور تمام شعبوں میں متاثرہ نظاموں کی بحالی میں مدد فراہم کرتا ہے۔ قابلِ عمل انٹیلی جنس اور رہنمائی کا مسلسل بہاؤ اسٹیک ہولڈرز کو اپنی تیاری مضبوط بنانے، نظامی خطرات کو کم کرنے اور ابھرتے ہوئے سائبر خطرات کا مؤثر انداز میں مقابلہ کرنے کے قابل بناتا ہے۔ یہ مشترکہ کوششیں ڈیجیٹل خلل کو کم کرنے، بحالی کے عمل کو تیز کرنے اور ہندوستان کے ڈیجیٹل ماحولیاتی نظام میں اعتماد کو مستحکم کرنے میں اہم کردار ادا کرتی ہیں۔

ہندوستان کی سائبر لچکدار حکمتِ عملی کے مرکز میں سی ای آر ٹی-اِن

سی ای آر ٹی-اِن فعال خطرات کی نشاندہی، تیز رفتار واقعہ جاتی ردِعمل اور وسیع پیمانے پر صلاحیت سازی کے ذریعے ہندوستان کے قومی سائبر دفاعی ڈھانچے کی بنیاد کے طور پر خدمات انجام دے رہا ہے۔ 2025 کے دوران اس کی کامیابیاں اس بات کی عکاس ہیں کہ ادارہ جاتی لچک کو مضبوط بنانے، اہم ڈیجیٹل بنیادی ڈھانچے کے تحفظ اور ہندوستان کے تیزی سے پھیلتے ہوئے ڈیجیٹل ماحولیاتی نظام پر اعتماد کو مستحکم کرنے کے لیے ایک مستقل، مربوط اور منظم کوشش جاری ہے۔

سی ای آر ٹی-اِن کی 2025 کی اہم کامیابیوں کا جائزہ

1۔نیشنل سائبر انسیڈنٹ رسپانس اور تھریٹ انٹیلی جنس

- سال 2025 کے دوران سی ای آر ٹی-اِن نے 29.44 لاکھ سے زائد سائبر واقعات سے مؤثر طور پر نمٹا، جس کے تحت 1,530 الرٹس، 390 ولنربلٹی نوٹس اور 65 ایڈوائزریز جاری کی گئیں۔ یہ اعداد و شمار بڑے پیمانے پر قومی سائبر رسپانس صلاحیت اور ادارہ جاتی تیاری کی عکاسی کرتے ہیں۔

- اس عرصے میں 29 عام کمزوریوں اور نمائشوں (سی وی ایز) کی نشاندہی کی گئی اور انہیں سی ای آر ٹی-اِن کی جانب سے باضابطہ طور پر شائع کیا گیا۔

2۔سائبر سیکیورٹی آڈٹ

- سی ای آر ٹی-اِن نے سرکاری، نیم سرکاری اور نجی شعبے کے انفارمیشن اینڈ کمیونیکیشن ٹیکنالوجی (آئی سی ٹی) نظاموں میں سائبر سیکیورٹی کو مضبوط بنانے کے مقصد سے 231 تصدیق شدہ سیکیورٹی آڈٹ تنظیموں کو پینل میں شامل کیا۔

- ان آڈٹس کی بڑی تعداد بینکنگ اور مالیاتی اداروں، بجلی اور توانائی، اور نقل و حمل کے شعبوں میں انجام دی گئی، جو ملک کے اہم اور حساس انفراسٹرکچر کے تحفظ پر خصوصی توجہ کی عکاسی کرتی ہے۔

3.صلاحیت سازی

- صلاحیت سازی کے میدان میں سی ای آر ٹی-اِن نے حکومت، پبلک سیکٹر انڈرٹیکنگز (پی ایس یوز) اور نجی شعبے کے اسٹیک ہولڈرز کے لیے 32 خصوصی تکنیکی تربیتی پروگرام اور 95 سائبر سیکیورٹی بیداری سیشنز منعقد کیے۔
- ان خصوصی پروگراموں کے ذریعے حکومت، پی ایس یوز اور صنعت سے وابستہ مجموعی طور پر 20,799 افسران اور سائبر سیکیورٹی کے پیشہ ور افراد کو تربیت فراہم کی گئی، جس سے قومی سطح پر مہارت اور تیاری میں نمایاں اضافہ ہوا۔

4.سائبر سیکیورٹی ڈرلز اور تیاری کی مشقیں

- سی ای آر ٹی-اِن نے 2025 کے دوران مختلف پیچیدگیوں کی حامل 122 سائبر سیکیورٹی مشقیں اور ڈرلز منعقد کیں، جن میں ٹیبل ٹاپ ایکسرسائزز بھی شامل تھیں۔ ان مشقوں میں دفاع، نیم فوجی دستے، خلائی شعبہ، جوہری توانائی، ٹیلی مواصلات (انٹرنیٹ سروس پرووائیڈرز)، مالیات، بجلی، تیل و قدرتی گیس، نقل و حمل، آئی ٹی/آئی ٹی ای ایس شعبہ اور ریاستی ڈیٹا سینٹرز سمیت سرکاری، نیم سرکاری اور نجی شعبوں کی تقریباً 1,570 تنظیموں نے شرکت کی۔

5.آگاہی کے اقدامات

سی ای آر ٹی-اِن نے مجموعی طور پر 95 بیداری سیشنز کا انعقاد کیا، جن سے 91,065 شرکاء مستفید ہوئے۔ ان میں اکتوبر 2025 میں منعقد ہونے والا نیشنل سائبر سیکیورٹی اویئرنیس منتھ (این سی ایس اے ایم) بھی شامل تھا۔

2025کے دوران، کمپیوٹر ایمرجنسی رسپانس ٹیم – انڈیا (سی ای آرٹی اِن) نے رپورٹس، وائٹ پیپرز، رہنما خطوط، ایڈوائزریز اور کمزوریوں (ولنریبیلٹی) سے متعلق نوٹس پر مشتمل ایک جامع سلسلہ شائع کیا، جس کا مقصد اداروں اور متعلقہ فریقین کو بروقت اور قابلِ عمل رہنمائی فراہم کرنا تھا، تاکہ سائبر خطرات کی پیشگی روک تھام اور سائبر لچک (ریزیلینس) کو مضبوط بنایا جا سکے۔

2025میں شائع ہونے والی رپورٹس اور رہنما خطوط

- اسمارٹ سٹی انفراسٹرکچر کے لیے سائبر سیکیورٹی رہنما خطوط (فروری 2025)
- سیٹلائٹ کمیونیکیشن کے لیے سائبر سیکیورٹی خطرات اور بہترین عملی طریقوں سے متعلق ایڈوائزری (فروری 2025)
- انڈیا رینسم ویئر رپورٹ (مارچ 2025)
- بینکنگ، فنانشل سروسز اور انشورنس (بی ایف ایس آئی) شعبے کے لیے ڈیجیٹل تھریٹ رپورٹ 2024 (اپریل 2025)
- وائٹ پیپر: ''غیر انسانی فضائی نظام (یون مینڈ ایئرکرافٹ سسٹمز – یو اے ایس) کو سائبر سیکیورٹی خطرات سے محفوظ رکھنے کے لیے اچھی عملی روایات'' (اپریل 2025)
- سافٹ ویئر بل آف میٹیریلز (ایس بی او ایم)، کوانٹم بل آف میٹیریلز (کیو بی او ایم) اور کرپٹوگرافک بل آف میٹیریلز (سی بی او ایم)، ہارڈویئر بل آف میٹیریل (ایچ بی او ایم)، اور آرٹیفیشل انٹیلیجنس بل آف میٹیریلز (اے آئی بی او ایم) ورژن 2 سے متعلق تکنیکی رہنما خطوط (جولائی 2025)
- جامع سائبر سیکیورٹی آڈٹ پالیسی رہنما خطوط (جولائی 2025)
- کوانٹم سائبر ریڈینس کی جانب منتقلی سے متعلق وائٹ پیپر (جولائی 2025)
- مائیکرو، اسمال اور میڈیم انٹرپرائزز (ایم ایس ایم ایز) کے لیے 15 بنیادی سائبر ڈیفنس کنٹرولز (ستمبر 2025)
- نیشنل سائبر سیکیورٹی اویئرنیس منتھ (این سی ایس اے ایم) اکتوبر 2025 کے دوران ''سائبر اسمارٹ کڈز: سرکشا گائیڈ'' کی اشاعت
- سینئر سٹیزنز کے لیے سائبر سیکیورٹی کی بہترین عملی روایات پر مبنی کتابچہ

سی ای آرٹی اِن کی 2025 کی کامیابیاں بھارت کے تیزی سے پھیلتے ہوئے ڈیجیٹل ایکو سسٹم کے تحفظ میں اس کے مرکزی کردار کی عکاسی کرتی ہیں۔ بڑے پیمانے پر صلاحیت سازی، سخت آڈٹس، مسلسل بیداری مہمات، اور مستقبل نگر تکنیکی و پالیسی فریم ورکس کی اشاعت کے ذریعے، سی ای آرٹی اِن نے حکومت، صنعت اور معاشرے میں ادارہ جاتی تیاری کو نمایاں طور پر مضبوط کیا ہے۔

سی ای آرٹی اِن کے زیرِ قیادت ادارہ جاتی فریم ورکس

قومی سائبر سیکیورٹی پالیسی کو عملی شکل دینے اور اسٹریٹجک مقاصد کو زمینی سطح پر نافذ کرنے کے لیے، سی ای آرٹی اِن متعدد خصوصی ادارہ جاتی فریم ورکس کی قیادت کرتا ہے۔ یہ نظام مختلف شعبوں، ریاستوں اور شہریوں کے مابین منظم ہم آہنگی، احتیاطی تحفظ، اور تیز رفتار ردِعمل کی صلاحیتیں فراہم کرتے ہیں۔

1سائبر سوچھتا کیندر (سی ایس کے)

سائبر سوچھتا کیندر (بوٹ نیٹ کلیننگ اینڈ میلویئر اینالیسس سینٹر) سی ای آرٹی اِن کے تحت قائم کیا گیا ہے تاکہ شہریوں میں سائبر حفظانِ صحت کو فروغ دیا جا سکے۔ یہ مرکز انٹرنیٹ سے منسلک آلات — جیسے کمپیوٹرز، موبائل فونز، آئی او ٹی ڈیوائسز اور گھریلو روٹرز — پر نظر رکھتا ہے جو میلویئر سے متاثر ہوتے ہیں۔یہ متاثرہ آلات کی صفائی کے لیے مفت ٹولز اور رہنمائی فراہم کرتا ہے، اور صنعت، اکیڈمیا اور انٹرنیٹ سروس پرووائیڈرز کے ساتھ قریبی تعاون کے ذریعے متاثرہ نظاموں کی نشاندہی اور صارفین کو آگاہ کرتا ہے۔ محفوظ آن لائن طرزِ عمل اور ذمہ دار ڈیجیٹل رویّوں کے فروغ کے لیے باقاعدہ بیداری مہمات بھی چلائی جاتی ہیں۔

دسمبر 2025 تک، سی ایس کے نے بھارت کی 98 فیصد ڈیجیٹل آبادی کا احاطہ کیا، اور بوٹ نیٹ و میلویئر انفیکشنز کے حوالے سے بڑے پیمانے پر اطلاعات جاری کیں۔ کلیدی شعبوں میں 1,427 اداروں کی شمولیت کے ساتھ، یہ میلویئر کی نشاندہی اور اس کے ازالے میں معاون رہا، جبکہ اس کے مفت بوٹ نیٹ ریموول ٹولز کے 89.55 لاکھ ڈاؤن لوڈز سی ایس کے کے شہری مرکوز، احتیاطی سائبر سیکیورٹی اقدامات کے کردار کو نمایاں کرتے ہیں۔

2.سیکیورٹی ایشورنس فریم ورک

سی ای آرٹی اِن ایک سیکیورٹی ایشورنس فریم ورک چلاتا ہے جس کا مقصد سرکاری اور اہم شعبہ جاتی نظاموں کی سیکیورٹی کو مضبوط بنانا ہے۔ اس فریم ورک کے تحت:

- مصدقہ آئی ٹی سیکیورٹی آڈٹ ادارے باقاعدہ آڈٹس انجام دیتے ہیں؛
- ولنریبیلٹی اسیسمنٹس اور پینیٹریشن ٹیسٹنگ کی جاتی ہے؛
- آڈٹ نتائج کا تجزیہ کر کے مشترکہ کمزوریوں کی نشاندہی کی جاتی ہے۔

ان مشاہدات کی بنیاد پر، سی ای آرٹی اِن محفوظ ڈیزائن رہنما خطوط جاری کرتا ہے اور بہترین عملی طریقوں کو فروغ دیتا ہے۔ اس فریم ورک کے تحت باقاعدہ آڈٹس مختلف شعبوں میں سائبر تیاری اور لچک کو نمایاں طور پر بہتر بناتے ہیں۔

3.نیشنل سائبر کوآرڈینیشن سینٹر (این سی سی سی)

نیشنل سائبر کوآرڈینیشن سینٹر، جسے سی ای آرٹی اِن نافذ کرتا ہے، میٹا ڈیٹا کی سطح پر سائبر اسپیس کی نگرانی کرتا ہے تاکہ ممکنہ سائبر سیکیورٹی خطرات کی نشاندہی اور صورتحال سے آگاہی حاصل کی جا سکے۔ یہ متعلقہ اداروں، ریاستی حکومتوں اور دیگر شراکت داروں کے ساتھ حقیقی وقت میں معلومات کے تبادلے کو ممکن بناتا ہے، جس سے بروقت احتیاطی اور ردِعمل اقدامات کیے جا سکتے ہیں۔

4.کمپیوٹر سیکیورٹی انسیڈنٹ رسپانس ٹیمز (سی ایس آئی آر ٹیز)

سی ای آرٹی اِن شعبہ جاتی اور ریاستی / مرکز کے زیرِ انتظام علاقوں کی سطح پر کام کرنے والی کمپیوٹر سیکیورٹی انسیڈنٹ رسپانس ٹیمز کے ایک نیٹ ورک کی نگرانی

کرتا ہے۔ شعبہ جاتی سی ایس آئی آر ٹیز مالیات، توانائی اور ٹیلی کام جیسے شعبوں کی معاونت کرتی ہیں، جبکہ ریاستی سی ایس آئی آر ٹیز متعلقہ ریاستی اور یو ٹی حکومتوں کے تحت کام کرتی ہیں۔

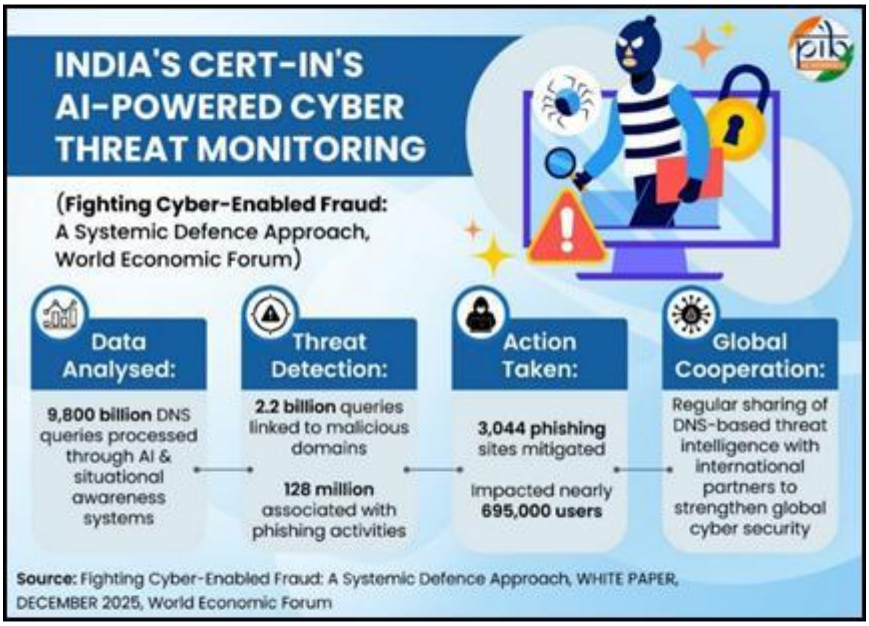
5۔سائبر کرائسس مینجمنٹ پلان (سی سی ایم پی)

سی ای آرٹی اِن نے سرکاری اداروں کے لیے سائبر کرائسس مینجمنٹ پلان بھی تیار کیا ہے، جو بڑے سائبر حملوں اور سائبر دہشت گردی کے واقعات کے دوران منظم رہنمائی فراہم کرتا ہے۔ یہ منصوبہ تیز رفتار ردِعمل، بحالی، اور ضروری خدمات کے تسلسل کو یقینی بنانے میں معاون ہے، خصوصاً اہم انفراسٹرکچر کے لیے۔

یہ تمام ادارہ جاتی فریم ورکس مجموعی طور پر حکومت اور معاشرے کی سطح پر ایک جامع نقطۂ نظر کو فروغ دیتے ہیں۔ روک تھام، تیاری، ردِعمل اور بحالی کو یکجا کر کے، یہ نظام اس امر کو یقینی بناتے ہیں کہ بھارت کا ڈیجیٹل ایکو سسٹم بدلتے ہوئے سائبر خطرات کے باوجود مضبوط، لچکدار اور محفوظ رہے۔ یہ تہہ دار ادارہ جاتی ڈھانچہ قومی تیاری کو مضبوط بنانے کے ساتھ ساتھ اہم انفراسٹرکچر اور شہریوں کے تحفظ کو بھی یقینی بناتا ہے۔

بھارت کی سائبر سیکیورٹی قیادت کا عالمی اعتراف

سی ای آرٹی اِن کی مسلسل داخلی کوششوں نے عالمی سطح پر بھی نمایاں پذیرائی حاصل کی ہے۔ اس کے عملی پیمانے، ٹیکنالوجی پر مبنی طریقۂ کار، اور باہمی تعاون پر مبنی سائبر گورننس پر زور نے بھارت کو بین الاقوامی سائبر سیکیورٹی ایکو سسٹم میں ایک معتبر اور ذمہ دار شراکت دار کے طور پر مستحکم کیا ہے۔



INDIA'S CERT-IN'S AI-POWERED CYBER THREAT MONITORING

(Fighting Cyber-Enabled Fraud: A Systemic Defence Approach, World Economic Forum)

Data Analysed:
9,800 billion DNS queries processed through AI & situational awareness systems

Threat Detection:
2.2 billion queries linked to malicious domains
128 million associated with phishing activities

Action Taken:
3,044 phishing sites mitigated
Impacted nearly **695,000 users**

Global Cooperation:
Regular sharing of DNS-based threat intelligence with international partners to strengthen global cyber security

Source: Fighting Cyber-Enabled Fraud: A Systemic Defence Approach, WHITE PAPER, DECEMBER 2025, World Economic Forum

- ورلڈ اکنامک فورم (ڈبلیو ای ایف) کی جانب سے شائع کردہ گلوبل سائبر سیکیورٹی آؤٹ لک 2025 میں، سی ای آرٹی اِن کو اے آئی پر مبنی صورتحال آگاہی نظاموں کے نفاذ کے لیے نمایاں کیا گیا ہے، جو بدنیتی پر مبنی ڈومینز اور فشنگ سرگرمیوں کے تجزیے اور نشاندہی میں معاون ہیں، نیز عالمی سطح پر حقیقی وقت میں تھریٹ انٹیلیجنس کے تبادلے کے لیے بھی اس کے کردار کو اجاگر کیا گیا ہے۔
- اپریل 2025 میں، سی ای آرٹی اِن نے ورلڈ اکنامک فورم اور یونیورسٹی آف آکسفورڈ کے اشتراک سے شائع ہونے والے “سائبر ریزیلینس کمپاس” پیپر میں تعاون کیا، جس میں سائبر لچک کے سات اہم شعبوں کی نشاندہی کی گئی۔
- فروری 2025 میں، سی ای آرٹی اِن فرانس کی نیشنل سائبر سیکیورٹی ایجنسی (اے این ایس ایس آئی) کی جانب سے شائع کردہ مصنوعی ذہانت سے متعلق مشترکہ اعلیٰ سطحی خطرات کے تجزیے کی رپورٹ “سائبر رسک پر مبنی نقطۂ نظر کے ذریعے قابلِ اعتماد اے آئی کی تشکیل” پر دستخط کرنے والے بین الاقوامی شراکت داروں میں شامل تھا۔ یہ رپورٹ قابلِ اعتماد اے آئی نظاموں، محفوظ اے آئی ویلیو چینز، اور اے آئی سے متعلق ابھرتے ہوئے سائبر خطرات سے نمٹنے کے لیے رسک پر مبنی طریقۂ کار کی وکالت کرتی ہے۔ یہ تمام اعترافات عالمی سطح پر سائبر سیکیورٹی اور اے آئی رسک گورننس کی تشکیل میں سی ای آرٹی اِن کے بڑھتے ہوئے اثر و رسوخ اور قیادت کو اجاگر کرتے ہیں۔ یہ سائبر لچک، تھریٹ انٹیلیجنس کے تبادلے، اور ذمہ دار اے آئی رسک گورننس سے متعلق عالمی مباحث میں سی ای آرٹی اِن کے ابھرتے ہوئے کردار کی عکاسی کرتے ہیں۔

نتیجہ

سائبر خطرات کی بڑھتی ہوئی پیچیدگی اور وسعت کے تناظر میں، سی ای آرٹی اِن بھارت کے سائبر سیکیورٹی ایکو سسٹم کی قیادت جاری رکھے ہوئے ہے۔ مسلسل سائبر خطرات کی نشاندہی اور ان کے ازالے کے ذریعے، سی ای آرٹی اِن نے قومی سطح پر سائبر لچک کو نمایاں طور پر مضبوط کیا ہے۔ اس کے اقدامات — جن میں ادارہ جاتی فریم ورکس، شعبہ جاتی اور ریاستی سی ایس آئی آر ٹیز، اور شہری مرکوز بیداری پروگرام شامل ہیں — بھارت کے آئی سی ٹی انفراسٹرکچر کے تحفظ اور صارفین کی سلامتی کے لیے ایک جامع اور مستقبل نگر نقطۂ نظر کی عکاسی کرتے ہیں۔

سی ای آرٹی اِن کی اے آئی پر مبنی اختراعات کو حاصل ہونے والا عالمی اعتراف بھی سائبر سیکیورٹی میں بھارت کی بڑھتی ہوئی قیادت کو نمایاں کرتا ہے۔ مجموعی طور پر، یہ مسلسل کوششیں حکومتِ ہند کے اس عزم کی توثیق کرتی ہیں کہ سائبر اسپیس کو محفوظ بنایا جائے اور تمام شہریوں کے لیے ایک محفوظ، قابلِ اعتماد اور محفوظ ڈیجیٹل مستقبل کو یقینی بنایا جائے۔

- **حوالہ جات**

وزارت الیکٹرانکس اور انفارمیشن ٹیکنالوجی
https://www.cert-in.org.in/

- https://www.cert-in.org.in/- Annual Report 2024
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2203387&reg=3&lang=1
- https://www.csk.gov.in/about.html
- https://www.cert-in.org.in/CSIRT.jsp
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2148943&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2109192&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2026677&reg=3&lang=2
- https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2115416&reg=3&lang=2
- UPI: https://www.npci.org.in/product/upi/product-statistics
- IMPS: https://www.npci.org.in/product/imps/product-statistics
- NETC: https://www.npci.org.in/product/netc/product-statistics
- DigiLocker: https://www.digilocker.gov.in/web/statistics
- https://www.cert-in.org.in/PDF/Guidelines_for_Smart_City_Infrastructure.pdf
- https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2024.pdf
- https://www.cert-in.org.in/PDF/Digital_Threat_Report_2024.pdf

- https://www.cert-in.org.in/PDF/CIWP-2025-0001.pdf
- https://www.cert-in.org.in/PDF/TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM_and_HBOM_ver2.0.pdf
- https://www.cert-in.org.in/ (Guidelines)
- https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2144023&reg=3&lang=2
- https://www.cert-in.org.in/PDF/Elemental_Cyber_Defense_Controls_for_MSME.pdf

وزارت مواصلات

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057035&reg=3&lang=2

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198285&reg=3&lang=2

وزارت داخلہ

htthttps://www.pib.gov.in/PressReleasePage.aspx?PRID=2197529&reg=3&lang=2

پی آئی بی ہیڈ کوارٹر:

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2

- https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=156294&ModuleId=3&reg=3&lang=1
- https://www.pib.gov.in/PressNoteDetails.aspx?ModuleId=3&NoteId=154788&reg=3&lang=1
- https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154912&ModuleId=3&reg=3&lang=1

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2206477&reg=3&lang=1

the420.in

- https://the420.in/cert-in-ai-praised-world-economic-forum-cyber-fraud-report

پی ڈی ایف دیکھنے کے لیے یہاں کلک کریں

***