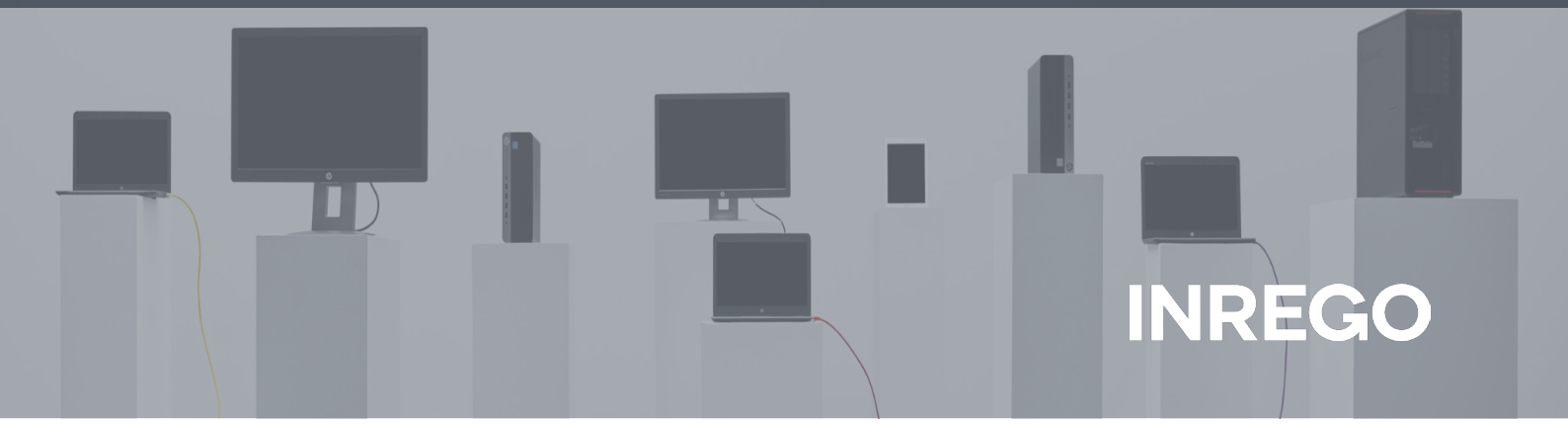

Organisationsnamn
INREGO

Land
Sverige

Industri:
IT

Lösning
Panda Adaptive Defense 360 + Panda Patch Management & Panda Advanced Reporting Tool

Licenser
220

"Utvecklingsmässigt är Pandas produkter en av de absolut bästa på marknaden"

Andreas

General Manager of Information and Communication Technology

Historia

Dagens kanske mest omtalade ämnen är miljö och klimatpåverkan. Med skrämmande siffror på koldioxidutsläpp och den stigande medeltemperaturen har detta tvingat både privatpersoner och företag att agera. Inte minst för vår miljö men också för att den allt mer medvetna konsumenten kräver allt mer klimatsmarta lösningar för att rättfärdiga sitt konsumerande.

Inrego, som är marknadsledande inom återanvändning och livscykelhantering av datorer, mobiler och andra IT-produkter, förstod detta långt innan det var en trend. År 1995 för att vara exakt. Inregos affärsidé går ut på att köpa använd IT-utrustning från organisationer för att testa att förbättra produkterna för att sedan se till att de kommer till nytta igen. Med hjälp av sina 160 anställda har Inrego hjälpt organisationer över hela Europa att stärka sitt hållbarhetsarbete.

Inregos mission är att minimera använd IT-utrustnings påverkan på miljön och deras vision är att förändra hur IT hanteras i samhället. Förra året hanterade Inrego 300 000 IT-produkter, som datorer, skärmar och mobiler och över 90 procent av utrustningen kunde gå till återanvändning, det vill säga säljas vidare på andrahandsmarknaden. Det innebär besparingar på både tusentals ton koldioxid och stora mängder andra resurser som metaller, vatten och kemikalier.

Inrego är Sveriges största återförsäljare av återanvända IT-produkter med tillhörande tjänster. Varje vecka levererar de över 5 000 datorer och andra IT-produkter till företag, skolor och kommuner.

Situation

Trots 160 anställda och en organisation som ständigt växer har Inrego varit besparade större säkerhetsrelaterade problem med sin interna IT. Innan Inrego valde Panda Adaptive Defense 360 och dess tilläggsmoduler Advanced Reporting Tool samt Panda Patch Management hade de ett traditionellt ”basic” virusskydd installerat på sina datorer vilket fungerade bra.

Efter 12 år på Inrego tog Andreas Ericson 2018 över som IT- och säkerhetschef för Inrego och valde att fokusera på att öka säkerheten i framförallt klientplattformen. Andreas vet att i princip alla organisationers största risk är deras användare och han ville därför minimera eventuella risker och dess efterföljder genom att byta till en säkerhetslösning som skyddar mot just det. Han tyckte att det var dags höja ambitionsnivån och gå ifrån det traditionella basic skyddet.

Lösning

Med Panda Adaptive Defense 360 får han precis det han efterfrågade, ett skydd som jobbar proaktivt. Precis som Andreas nämnde när vi talades vid så är användarna en av de största utmaningarna en organisation har.

Med hjälp av Panda Adaptive Defense 360 minimeras risken för IT-säkerhetsincidenter då den initialt blockerar all okänd programvara om den inte i förväg ”whitelistats” eller godkänts av Pandas centrala granskning.

Säkerhetsmodellen bygger på tre principer: kontinuerlig övervakning av applikationer på företagets datorer och servrar, automatisk klassificering och maskininlärning. Dessa skyddar klienten/servern mot kända och okända attacker via exempelvis epost eller internet. Panda Adaptive Defense 360 är även den första lösningen som ger en kombination av Endpoint Protection (EPP) och Endpoint Detection & Response (EDR) i samma lösning.

En annan mycket vanlig utmaning inom organisationer är saknade uppdateringar. En vanlig missuppfattning är att Microsoft/Windows och andra program håller sig uppdaterade automatiskt. Det är sällan fallet.

Opatchade operativsystem och mjukvara från tredje part ger en perfekt grund för attacker och exploits att dra fördel av kända sårbarheter, vars patchar varit tillgängliga i veckor (eller till och med månader i vissa fall) innan intrånget.

Syftet med Panda Patch Management är att förhindra incidenter och systematiskt minska attackytan som skapas av programvarusårbarheter. Hantering av patchar och uppdateringar med lättanvända verktyg för realtidshantering som gör det möjligt för organisationer att ligga steget före sårbarhetsutnyttjande attacker.

Andreas valde att även använda sig av Patch Management, trots att Inrego redan hade en annan specialiserad programvara för ändamålet. Detta då Pandas Patch Management både var snäppet vassare rent tekniskt och även innebar en förenkling i användandet samt dessutom innebar en besparing genom att inte behöva ytterligare en separat programvara.

Andreas lade även till Advanced Reporting Tool som en extra tilläggsmodul med funktioner som gör det möjligt att få varningar i realtid om potentiella hot. Dessutom ger den en centraliserad visualisering av säkerhetsstatusen för programvarans sårbarheter, programvaruproblem, uppdateringar och icke-supporterad (EOL)3 -programvara, inuti och utanför företagsnätverket.

Avancerad Reporting Tool gör det möjligt för automatiserad lagring och korrelation av informationen relaterad till processutförande och dess sammanhang extraherad av Panda Adaptive Defense 360 från endpoints.

INREGO

Huvudsaklig nytta:

Panda Adaptive Defense 360:

- EDR-teknik med komplett skydd mot zero-days attacker

- Full EPP-kapacitet

- 100% attesteringstjänst - validerar alla processer som körs

- Minskar skriptbaserad och skadlig programvara

- Close technical support by qualified technicians

- Användarvänlig agent

Panda Patch Management:

- Granska, övervaka och prioritera operativsystem och programuppdateringar.

- Förhindra incidenter, systematiskt minska attackytan som skapas av programvarusårbarheter.

- Begränsa och mildra sårbarhetsutnyttjande attacker med omedelbara uppdateringar.

- Minska operativkostnader.

INREGO

Huvudsaklig nytta:

Panda Advanced Reporting Tool:

- Lagrar och korrelerar information om endpoint-aktivitet

- Övervakning och visualisering av realtids- och retrospektiv data, vilket gör det möjligt för organisationer att analysera säkerhetsindikatorer och användning av företagets resurser, samt att upptäcka potentiella risker, misstänkta beteenden eller attacker

- Avancerat rapporteringsverktyg innehåller instrumentpaneler med viktiga indikatorer, sökalternativ och förkonfigurerade varningar för tre specifika områden:

- Säkerhetsincidenter
- Tillgång till kritisk information
- Användning av applikations- och nätverksresurser

Denna information gör det även möjligt för Advanced Reporting Tool att automatiskt generera säkerhetsinformation och tillhandahålla verktyg som möjliggör för organisationer att fastställa attacker och ovanligt beteende, oavsett ursprung, liksom att upptäcka internt missbruk av företagets system och nätverk.

Tilläggsmodulen ger också organisationer sök-, utforsknings- och analysfunktioner, och erbjuder IT- och säkerhetsinsikter utan att behöva investera i infrastruktur, installationer eller underhåll.

Slutsats

Inrego som ännu inte har ställts inför några större utmaningar inom den interna IT-säkerheten var ute efter proaktiva lösningar för att förhindra att detta sker i framtiden. Det var i maj förra året som Andreas tog beslutet att köpa in Pandas säkerhetslösningar och när vi talas vid så är han väldigt nöjd med både Pandas produkter och installationerna av dem. ”Bytet ifrån vår tidigare lösning till Pandas produkter var både enkelt och smidigt” säger Andreas själv och han avslutar även vårt samtal med att berömma våra produkter genom att säga att de utvecklingsmässigt är en av de absolut bästa på marknaden. Andreas är med andra ord väldigt nöjd med Panda och vi på Panda är väldigt nöjda med att ha kunder som Inrego.