ZTE

leading 5G innovations

ZTE

leading 5G innovations

WHITE PAPER SULLA CYBERSECURITY DI ZTE

FORNIRE AI CLIENTI IN OGNI FASE UNA GARANZIA
DI SICUREZZA PER PRODOTTI E SERVIZI.
SICUREZZA NEL DNA, FIDUCIA ATTRAVERSO LA TRASPARENZA.

ZTE

leading 5G innovations

WHITE PAPER SULLA CYBERSECURITY DI ZTE

FORNIRE AI CLIENTI IN OGNI FASE UNA GARANZIA
DI SICUREZZA PER PRODOTTI E SERVIZI.
SICUREZZA NEL DNA, FIDUCIA ATTRAVERSO LA TRASPARENZA.

ZTE

Scritto dall'autore:

Questo white paper descrive l'opinione, i principi, le strategie e le prassi di ZTE in termini di sicurezza informatica. Questo documento è stato sviluppato congiuntamente da molti colleghi.

Mi piacerebbe ringraziare chi ha offerto un contributo importante alla stesura di questo documento: Cao Kunpeng, Cheng Junhua, Chi Yifei, Gao Ruixin, He Ying, Hua Guohong, Li Rongkun, Liu Risheng, Liu Yan, Liu Yan, Long Hao, Xu Guorong, Meng Zhuli, Nie Yongli, Ping Li, Song Weiqiang, Ma Zhiyuan, Wang Huagang, Wang Lin, Wang Yuzhong, Wei Yinxing, Yang Tiejian, Zhang Can, Zhang Jie, Zhang Rui, Zhao Shanhong, Zheng Jun, Zhou Jihua e altri che hanno contribuito direttamente o indirettamente a questo white paper.

Zhong Hong
Chief Security Officer di ZTE Corporation

Indice

ZTE

Premessa

Il ciberspazio è diventato parte integrante della società moderna, influenzando tutti gli aspetti della vita quotidiana delle persone. A causa della natura ampia e aperta della tecnologia, il ciberspazio è un obiettivo facile, facilmente attaccato o danneggiato a causa della natura asimmetrica delle minacce e delle difese cibernetiche e delle vulnerabilità intrinseche del ciberspazio. Strettamente correlato a tutti i sistemi e le persone che fanno affidamento sulle reti, la sicurezza informatica è già diventata una preoccupazione per governi, operatori e utenti in tutto il mondo.

Le apparecchiature di telecomunicazione e i sistemi informatici sono le due principali piattaforme infrastrutturali di supporto del ciberspazio. In qualità di fornitore di soluzioni di telecomunicazioni integrate per i mercati internazionali, ZTE ha insistito sui seguenti principi in termini di sicurezza informatica:

La sicurezza informatica è una delle massime priorità delle business unit responsabili dello sviluppo e della consegna dei prodotti ZTE e, di conseguenza, ZTE ha stabilito una struttura di governance della cybersecurity olistica alla base della strategia di sviluppo dell'azienda. Il piano è supportato da leggi, regolamenti e norme pertinenti, promuovendo al contempo una buona consapevolezza della sicurezza per tutti i dipendenti e sottolineando l'importanza della sicurezza nell'intero processo end-to-end.
La società attribuisce grande importanza ai valori di sicurezza dei clienti, si attiene alle leggi e ai regolamenti pertinenti nell'ambito della sicurezza informatica e garantisce la consegna end-to-end di prodotti e servizi sicuri e affidabili.
ZTE continua a comunicare e a collaborare con operatori, agenzie di regolamentazione, partner e altre parti interessate in modo aperto e trasparente in relazione al miglioramento continuo delle nostre prassi di sicurezza informatica. In conformità con le leggi e i regolamenti, ZTE rispetta i diritti e gli interessi legittimi degli utenti e degli utenti finali, e continua a innovare e migliorare la nostra gestione e le prassi tecniche. In definitiva, ZTE si impegna a fornire ai clienti prodotti e servizi sicuri e affidabili, creando al contempo un ambiente cyber sicuro insieme a tutte le parti interessate e mantenendo un solido ordine di sicurezza per il ciberspazio.

RIEPILOGO ESECUTIVO

L'era 5G è cominciata. Tecnologie come il cloud computing, l'Internet of Things (IoT), i big data e l'intelligenza artificiale stanno spopolando sul mercato. Queste nuove tecnologie stanno determinando una nuova rivoluzione del settore e preoccupazioni di cybersecurity sempre più gravi.
Insistendo su apertura, trasparenza e fiducia, ZTE implementa la propria governance sulla sicurezza informatica attraverso un approccio top-down.

L'era 5G è cominciata. Tecnologie come il cloud computing, l'Internet of Things (IoT), i big data e l'intelligenza artificiale stanno spopolando sul mercato. Queste nuove tecnologie stanno determinando una nuova rivoluzione del settore e preoccupazioni di cybersecurity sempre più gravi, con crescenti minacce alla sicurezza informatica e crimini informatici che dilagano in tutto il mondo. Il rapporto Verizon Data Breach Investigations 2018[1] elaborato in merito alle situazioni di sicurezza informatica in molte industrie in tutto il mondo. Il rapporto sostiene oltre 53.000 incidenti di sicurezza informatica e sono stati segnalati durante l'inchiesta 2216 casi di violazioni dei dati confermati nel 2018. I sistemi informatici possono presentare numerose vulnerabilità di sicurezza, da febbraio 2019 le vulnerabilità esposte CVE[2] hanno raggiunto 112364, di cui il 13,5% erano vulnerabilità critiche e il 23,0% vulnerabilità alte.

Le apparecchiature e i sistemi di telecomunicazione composti da apparecchiature per le comunicazioni di informazioni sono fondamentali per la crescita del ciberspazio. A causa della natura asimmetrica delle minacce alla sicurezza e delle difese e delle vulnerabilità intrinseche esistenti nel sistema, queste infrastrutture di comunicazione sono facilmente attaccate e danneggiate, mettendo in pericolo l'intero sistema. Governi, operatori e fornitori di servizi esprimono tutti le loro preoccupazioni in merito alla sicurezza informatica, ad esempio integrità dei prodotti, assenza di backdoor, sicurezza delle lorosupply chain e protezione dei dati personali.

Insistendo su apertura, trasparenza e fiducia, ZTE implementa la propria governance sulla sicurezza informatica attraverso un approccio top-down. Basato su un modello di governance della sicurezza a "tre linee di difesa", ZTE non solo integra le proprie politiche di sicurezza in ogni fase del ciclo di vita del prodotto, ma implementa anche il meccanismo di garanzia della sicurezza informatica durante tutto il ciclo di vita del prodotto, assicurando così che R&S, supply chain e produzione del prodotto, servizi di in egneria, gestione di incidenti di sicurezza, verifiche indipendenti e audit siano tutti inclusi. Sviluppando linee di base per la sicurezza informatica, sostenute da processi e implementando la gestione a ciclo chiuso per la sicurezza informatica, ZTE consente la consegna sicura end-to-end di prodotti e servizi.

1 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

2 https://www.cvedetails.com/

FOCUS E IMPEGNI DAL TEAM LEADERSHIP DI ZTE

ZTE attribuisce grande importanza ai valori di sicurezza dei nostri clienti, si attiene alle leggi e ai regolamenti pertinenti nell'ambito della sicurezza informatica e garantisce la consegna end-to-end di prodotti e servizi sicuri e affidabili. La sicurezza informatica è una delle massime priorità per le business unit responsabili dello sviluppo e della consegna dei prodotti ZTE. Abbiamo stabilito una struttura governance olistica della cybersecurity nel piano di sviluppo strategico della società, tenendo conto delle leggi, dei regolamenti e delle norme pertinenti, promuovendo così una buona consapevolezza della sicurezza per tutti i dipendenti e sottolineando la sicurezza dell'intero processo.

ELEMENTI DELLA STRATEGIA DI SICUREZZA INFORMATICA DI ZTE

Il programma di garanzia della sicurezza informatica end-to-end di ZTE aderisce a sei elementi chiave: Standardizzazione, Implementazione rigorosa, Tracciabilità, Supervisione efficace, Trasparenza totale e Affidabilità.

Standardizzazione: *Il rispetto delle regole e norme globali, sviluppato in una serie di politiche, norme, processi e linee guida per la sicurezza informatica per aiutare a modellare e guidare il business.*

Implementazione rigorosa: *La sicurezza informatica all'interno di ciascuna business unit è implementata in modo rigoroso in conformità con i regolamenti, supportata da un sistemadi responsabilità e da una "Product Security Red Line".*

Supervisione efficace: *Miglioramento della supervisione e della gestione mediante l'attuazione di un modello di governance della sicurezza a tre linee di difesa.*

Tracciabilità: *Attività di sviluppo del prodotto end-to-end supportate da registrazioni probatorie e tracciabilità, garantendo che i problemi possano essere rilevati e individuati rapidamente.*

Trasparenza totale: *Aprire i nostri processi e procedure per consentire a clienti, governi e altre parti interessate di convalidare la nostra sicurezza informatica. I clienti possono convalidare le attività di sicurezza in loco. I problemi di sicurezza e le vulnerabilità sono divulgati in modo trasparente. Le patch vengono rilasciate tempestivamente.*

Affidabilità: *Ottenere la fiducia dei clienti attraverso attività di governance della sicurezza aperte e trasparenti e la certificazione e verifica di sicurezza di terze parti.*

UN MODELLO DI GOVERNANCE DELLA SICUREZZA A TRE LINEE DI DIFESA

Dal punto di vista organizzativo, ZTE implementa un modello di governance della sicurezza a tre linee di difesa per garantire la sicurezza dei prodotti e dei servizi da più punti di vista. Nella prima linea di difesa, ciascuna business unit è responsabile dell'implementazione dell'autocontrollo sulla sicurezza informatica, utilizzando procedure e processi di best practice. La divisione Sicurezza prodotti della società è la seconda linea di difesa, responsabile per le valutazioni e la supervisione indipendente della sicurezza. Infine, la divisione Controllo interno e audit di ZTE come terza linea di difesa controlla e verifica l'efficacia della prima e della seconda linea di difesa. Allo stesso tempo, ZTE accetta i controlli di sicurezza organizzati dai clienti e da terze parti esterne.

SVILUPPO DI TEAM DI SICUREZZA SPECIALIZZATI

ZTE organizza diversi tipi di formazione sulla sicurezza per aumentare la consapevolezza della sicurezza e accrescere le competenze di sicurezza professionale, che possono assumere la forma di seminari di alto livello, corsi di formazione manageriale, formazione sulla consapevolezza per tutti i dipendenti, formazione sulla progettazione sicura, formazione sui test di penetrazione e competizioni di codifica sicure.
Tale formazione non solo migliora la sicurezza dei prodotti della società, ma favorisce anche una cultura della cybersecurity all'interno della società. ZTE attribuisce grande importanza alla coltivazione di talenti in sicurezza professionale. Attualmente, ZTE ha più di 30 dipendenti che sono stati certificati da organizzazioni internazionali come CISSP, CISA, CSSLP, CEH, CCIE, CISAW e C-CCSK per le loro capacità di sicurezza. ZTE vanta capacità di sicurezza solide in termini di architettura di sicurezza matura, principi di progettazione sicuri, test di penetrazione completi, audit di sicurezza e gestione della sicurezza.

CONSEGNA SICURA END-TO-END

La sicurezza di ogni singola parte del sistema potrebbe influire sull'intero sistema. Tuttavia, la forza di un intero sistema è determinata dalla parte più debole. La governance della sicurezza di ZTE include R&S, supply chain, servizi di ingegneria, gestione degli incidenti e tutte le funzioni di supporto. Prendiamo ad esempio la R&S, i controlli di sicurezza sono inclusi nelle fasi dei requisiti di sicurezza, progettazione sicura, codifica sicura, test di sicurezza, recapito corretto e operazioni e manutenzione sicure (O&M). Anche la sicurezza delle componenti di terzi è presa in considerazione. Prendiamo la Supply Chain come altro esempio, le attività di sicurezza riguardano acquisti, produzione, magazzino, spedizione e consegna finale.

RISPOSTA AGLI INCIDENTI DI SICUREZZA INFORMATICA

Il Team PSIRT (Product Security Incident Response Team) di ZTE identifica e analizza gli incidenti di sicurezza, tiene traccia dei processi di gestione degli incidenti e comunica strettamente con gli stakeholder interni ed esterni per divulgare tempestivamente le vulnerabilità della sicurezza, garantendo così che attenuiamo gli effetti negativi degli incidenti di sicurezza. In qualità di membro del Forum di Incident Response and Security Teams (FIRST) e della CVE Numbering Authority (CNA), ZTE sta collaborando con i clienti e le parti interessate in modo trasparente per garantire che facciamo tutto il possibile per proteggere le reti dei nostri clienti

VALUTAZIONI E VERIFICA INDIPENDENTI

In virtù del modello di governance della sicurezza a tre linee di difesa, vengono eseguite valutazioni e verifiche della sicurezza indipendenti appartenenti alla seconda linea di difesa per valutare e supervisionare le prassi di sicurezza di prima linea. Basato su principi di controllo del rischio, le valutazioni e le verifiche di sicurezza indipendenti rivedono la sicurezza informatica da più punti di vista. Viene implementato un meccanismo di supervisione e controllo per ridurre ulteriormente i rischi per la sicurezza. La gestione a ciclo chiuso viene utilizzata per tracciare i problemi identificati e assicurare che siano risolti. Tutte queste misure assicurano che la governance della sicurezza informatica di ZTE continui a migliorare costantemente.

AUDIT DELLA SICUREZZA

Gli audit di sicurezza di ZTE valutano in modo indipendente la robustezza, la solidità e l'efficacia del nostro sistema di garanzia della sicurezza informatica. Gli aspetti da controllare comprendono l'organizzazione e il funzionamento, i processi di gestione dei rischi, le attività di controllo e la supervisione interna. Gli audit di sicurezza della società coprono il processo di garanzia della cybersecurity end-to-end, che comprende governance generale della sicurezza informatica, sicurezza R&S, sicurezza della supply chain, sicurezza dell'erogazione dei servizi, risposta agli incidenti di sicurezza e valutazioni indipendenti della sicurezza. L'obiettivo è realizzare la supervisione e la trasparenza per l'intero programma di sicurezza informatica.

CERTIFICAZIONE E COLLABORAZIONE DI SICUREZZA DI TERZE PARTI

Nel 2005, ZTE ha superato per la prima volta la certificazione ISO27001 Information Security Management System (ISMS). Questa certificazione deve essere rivista ogni anno e copre tutte le attività ZTE, con il nostro ultimo certificato rilasciato nel 2018. Nel 2017, ZTE ha superato la certificazione del sistema di gestione della sicurezza della supply chain ISO 28000. Ad oggi, le 12 categorie di prodotti ZTE hanno superato la certificazione Common Criteria (CC) (che è uno standard internazionale per la certificazione della sicurezza del prodotto).
I prodotti che hanno ottenuto la certificazione CC includono diversi prodotti e apparecchiature mainstream, per esempio, apparecchiature per reti core e reti di accesso, apparecchiature di trasporto ottico, apparecchiature per la gestione della rete, router e controller della stazione di base.

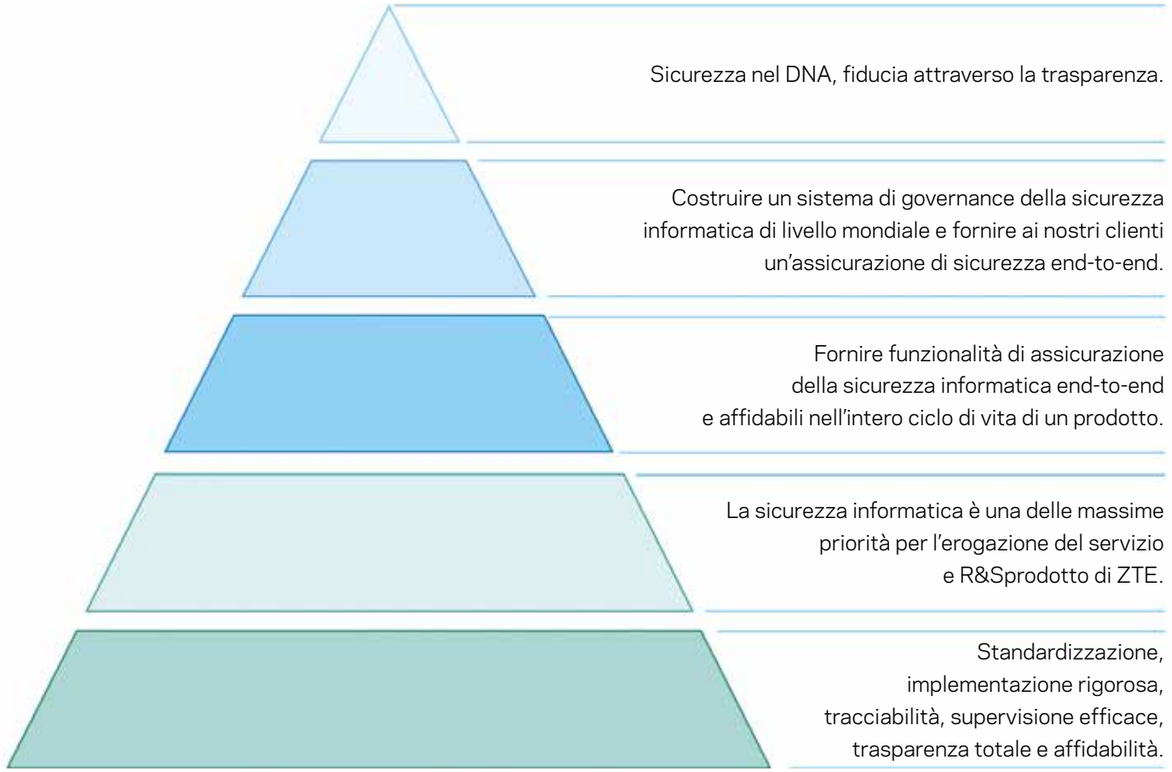
ZTE collabora, inoltre, attivamente con diverse organizzazioni di terze parti per valutare la sicurezza informatica dell'azienda. Ad esempio, alle terze parti sono affidati audit del codice sorgente, valutazioni della progettazione della sicurezza e test di penetrazione.

Basato sulla visione di ZTE per la sicurezza informatica, che è "Sicurezza nel DNA, fiducia attraverso la trasparenza", l'obiettivo finale di ZTE è fornire ai nostri clienti soluzioni affidabili e una sicurezza end-to-end per l'intero ciclo di vita di un prodotto. La società continua a comunicare e collaborare con agenzie di regolamentazione, clienti, partner e altre parti interessate in modo aperto e trasparente per creare e migliorare insieme un ecosistema sicuro per la sicurezza informatica.

Questo white paper illustra la strategia, la visione, la missione, l'obiettivo e le tattiche di ZTE in termini di sicurezza informatica, introduce le pratiche di cybersecurity end-to-end dell'azienda, inclusa la costruzione del suo modello di governance della sicurezza a tre linee di difesa, sicurezza per R&S, supply chain, consegna e informazioni, gestione degli incidenti di sicurezza, gestione della continuità operativa, valutazione indipendente della sicurezza e controllo della sicurezza. Il documento si conclude con una panoramica delle pietre miliari di ZTE nel campo della sicurezza informatica.

STRATEGIA DI SICUREZZA INFORMATICA ZTE

Le reti di telecomunicazioni sono classificate dai paesi come infrastrutture di rete critiche (CNI). Tutti i servizi (compresi i servizi pubblici) in esecuzione su queste reti sono considerati cruciali per il normale funzionamento di un paese. Operatori, governi e utenti attribuiscono un valore elevato alla sicurezza delle reti di telecomunicazione. ZTE attribuisce, inoltre, grande importanza alla sicurezza di queste reti CNI e ha formulato una strategia di sicurezza informatica che garantisce che la sicurezza sia una delle massime priorità in termini di R&S e consegna dei prodotti dell'azienda.



VISIONE: SICUREZZA NEL DNA, FIDUCIA ATTRAVERSO LA TRASPARENZA

Piuttosto che essere una funzionalità aggiuntiva, la sicurezza è vista come una proprietà intrinseca dei nostri prodotti. ZTE integra la sicurezza informatica nella nostre operazioni, la nostra organizzazione, i nostri processi, le nostre tecnologie e la nostra cultura. ZTE è disposta a condividere con i clienti i dettagli relativi all'adempimento dei prodotti e alla sicurezza dei processi. ZTE ritiene che la fiducia dei clienti si costruisca attraverso l'apertura e la trasparenza. ZTE consentirà ai clienti di controllare il codice sorgente dei nostri prodotti e la documentazione di progetto, di avere una panoramica dei sistemi operativi, effettuare test completi e comprendere le misure di sicurezza che ZTE ha intrapreso nello sviluppo dei nostri prodotti.

MISSIONE: COSTRUIRE UNA GOVERNANCE DELLA SICUREZZA INFORMATICA DI LIVELLO MONDIALE E FORNIRE AI NOSTRI CLIENTI UN'ASSICURAZIONE DI SICUREZZA END-TO-END

Il senior management di ZTE si impegna a continuare a investire risorse per costruire un sistema di governance della sicurezza di livello mondiale, che include l'ottimizzazione della struttura organizzativa, risorse umane, processi e procedure e tecnologie innovative per garantire che l'attività dell'azienda proceda in modo sicuro e che i clienti ottengano una garanzia della sicurezza end-to-end.

OBIETTIVO: FORNIRE FUNZIONALITÀ DI ASSICURAZIONE DELLA SICUREZZA INFORMATICA END-TO-END E AFFIDABILI NELL'INTERO CICLO DI VITA DI UN PRODOTTO

ZTE fornirà sicurezza informatica end-to-end basata sui requisiti e le aspettative dei clienti. In conformità con le leggi e i regolamenti pertinenti, gli standard di sicurezza e i principi di best practice, ZTE proteggerà reti, apparecchiature, applicazioni e dati da attacchi, danni e accessi non autorizzati fornendo soluzioni di sicurezza informatica end-to-end attraverso la propria organizzazione, i relativi processi e le tecnologie. ZTE è impegnata nella creazione di una solida struttura di governance della sicurezza informatica e nella creazione di un meccanismo di garanzia della sicurezza end-to-end per tutte le fasi del ciclo di vita del prodotto, ad esempio, R&S del prodotto, supply chain e produzione, consegna ingegneria, gestione degli incidenti di sicurezza, valutazione e audit. Costruendo un modello di governance per la sicurezza a tre linee di difesa, stabilendo linee di base per la sicurezza informatica, sviluppando processi per la gestione della sicurezza, implementando la gestione a ciclo chiuso per la sicurezza informatica e fornendo funzionalità affidabili di sicurezza informatica, ZTE creerà fiducia e garantirà che il nostro processo di sicurezza informatica sia di livello mondiale. Per migliorare la fiducia dei clienti nelle funzionalità di sicurezza informatica di ZTE, garantiremo il controllo dell'integrità del prodotto, l'assenza di backdoor, supply chain sicura e protezione dei dati personali, per citare solo alcuni esempi.

STRATEGIA: LA SICUREZZA INFORMATICA È UNA DELLE MASSIME PRIORITÀ PER LE BUSINESS UNIT RESPONSABILI DELLO SVILUPPO E DELLA CONSEGNA DEI PRODOTTI ZTE.

In ZTE, la sicurezza informatica avrà sempre la massima priorità, indipendentemente dalle funzioni e/o dai progressi richiesti. Rispetto ai principali punti decisionali nei processi di R&S e ingegneria, ZTE attribuisce la massima priorità alla sicurezza informatica nell'adozione di qualsiasi decisione.

TATTICA: STANDARDIZZAZIONE, IMPLEMENTAZIONE RIGOROSA, TRACCIABILITÀ, SUPERVISIONE EFFICACE, TRASPARENZA TOTALE E AFFIDABILITÀ.

Standardizzazione: *Rispettare le regole e gli standard e sviluppare politiche di sicurezza informatica e specifiche di processo di livello mondiale per ogni prodotto e ogni processo. Formulare una serie di politiche, standard, processi e procedure e linee guida in materia di sicurezza informatica.*

Implementazione rigorosa: *Misurare e monitorare il lavoro quotidiano di ciascuna business unit per garantire una conformità rigorosa alle normative raccomandate. Rafforzare l'implementazione costruendo un sistema di responsabilità e rilasciando la "Product Security Red Line".*

Supervisione efficace: *Rafforzare la supervisione e la gestione attraverso un modello di governance della sicurezza a tre linee di difesa. Assicurarsi che la divisione di regolamentazione attui gli audit di processo e controlli lo stato di implementazione degli standard di sicurezza, con i risultati dell'audit e lo stato di implementazione degli standard di sicurezza segnalati al Cyber Security Committee della società.*

Tracciabilità: *Assicurarsi che i componenti e l'ubicazione di un prodotto possano essere manutenuti e gestiti. Tutte le attività che implicano la sicurezza informatica devono essere rintracciabili attraverso registri e tracciabili attraverso prove, in modo da poter rilevare e individuare rapidamente i problemi.*

Trasparenza totale: *Aprire le attività end-to-end di ZTE in materia di sicurezza informatica a clienti, governi e altre parti interessate. I clienti hanno accesso ad attività quali il controllo del codice, la divulgazione completa di eventuali problemi di sicurezza, vulnerabilità e patch in corso. La creazione di un laboratorio di sicurezza all'estero in cui i clienti possono verificare sistemi, codice sorgente e documentazione tecnica dei prodotti ZTE. In quanto organizzazione CVE, ZTE offre alle parti interessate l'accesso ai propri processi di gestione della sicurezza per le vulnerabilità attraverso politiche standard sull'esposizione alla vulnerabilità.*

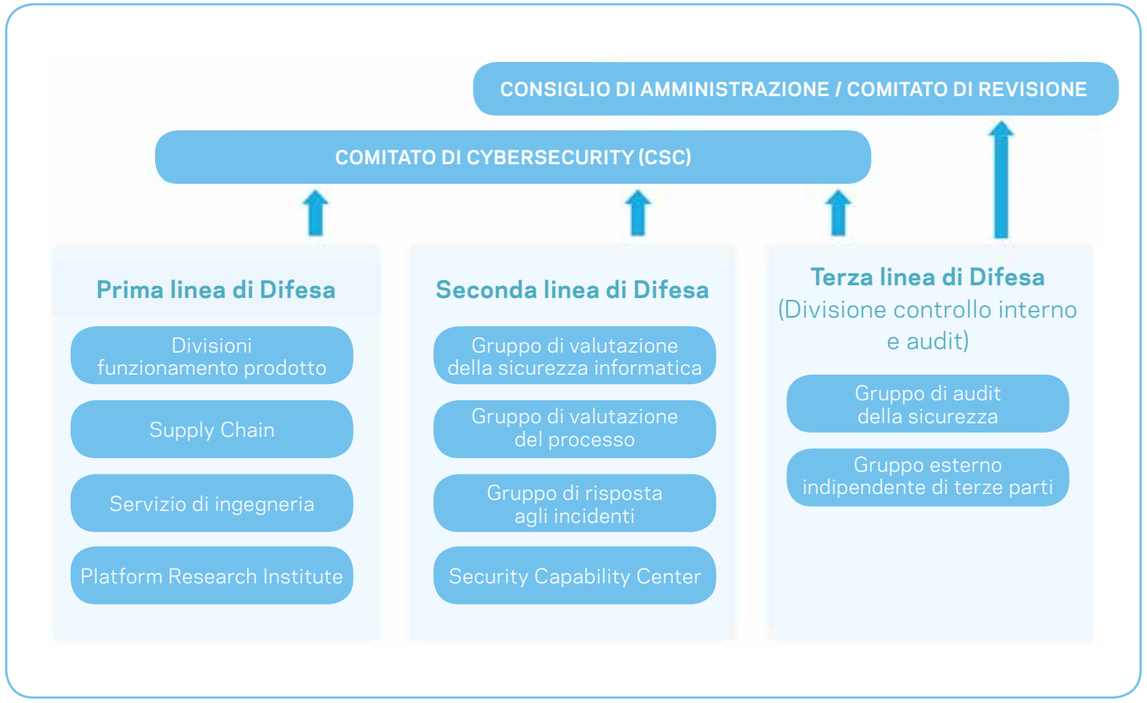
Affidabilità: *Ottenere la fiducia dei clienti attraverso attività di governance della sicurezza aperte e trasparenti e la certificazione della sicurezza di terze parti. ZTE instaura una stretta collaborazione con i clienti, le terze parti e le agenzie di regolamentazione per effettuare costantemente audit del codice sorgente, revisione della progettazione della sicurezza e audit presso i fornitori.*

PRASSI DI SICUREZZA INFORMATICA END-TO-END

ZTE rispetta le leggi e i regolamenti applicabili in materia di sicurezza informatica, in relazione agli standard internazionali e nazionali, e si basa sulle migliori prassi di sicurezza del settore. ZTE ricerca le prassi di sicurezza da aziende leader, al fine di migliorare continuamente le nostre prassi di sicurezza, rafforzando costantemente le nostre capacità di cybersecurity per fornire ai clienti prodotti e servizi sicuri e affidabili.

ARCHITETTURA DELLA GOVERNANCE PER LA SICUREZZA INFORMATICA BASATA SU TRE LINEE DI DIFESA

ZTE ha creato un'architettura organizzativa basata su tre linee di difesa per promuovere la governance della sicurezza informatica. Questa struttura risolve i conflitti di interesse utilizzando i meccanismi organizzativi ed evita i rischi delle business unit in prima linea che sacrificano i requisiti di sicurezza per il progresso del mercato, spinti dalla domanda di prodotti e servizi. La struttura segue anche il principio del controllo del rischio, garantendo la sicurezza informatica da vari punti di vista e livelli multipli attraverso l'auto-ispezione da parte delle business unit, la valutazione indipendente della sicurezza della seconda linea di difesa e l'audit di sicurezza della terza linea di difesa.



CONSIGLIO DI AMMINISTRAZIONE/COMITATO DI REVISIONE

Il Consiglio di amministrazione autorizza il Comitato di Cybersecurity (CSC) a svolgere attività di governance della sicurezza informatica. Il Consiglio di amministrazione o il Comitato di revisione riesamina anche le relazioni di audit della sicurezza consegnate dalla Divisione Controllo interno e audit.
Ciò garantisce che i prodotti e le soluzioni ZTE ricevano il massimo livello di impegno a livello di consiglio di amministrazione.

COMITATO DI CYBERSECURITY (CSC)

La principale organizzazione decisionale responsabile del lavoro di sicurezza informatica di ZTE.
Il Comitato di Cybersecurity formula strategie di cybersecurity e garantisce risorse, determina la direzione strategica e l'obiettivo del lavoro di cybersecurity, rivede i piani di sicurezza informatica e decide sulle principali questioni legate alla sicurezza informatica.

PRIMA LINEA DI DIFESA (BUSINESS UNIT)

Ogni business unit rappresenta la prima linea di difesa per la governance della cybersecurity. Ogni business unit realizza l'autocontrollo della sicurezza informatica attraverso i processi e le procedure approvate dal CSC per l'auto-progettazione, l'auto-esecuzione, l'auto-rilevazione e l'auto-miglioramento della sicurezza informatica.

SECONDA LINEA DI DIFESA (DIVISIONE SICUREZZA PRODOTTO)

La Divisione Sicurezza prodotto è la seconda linea di difesa per la governance della sicurezza informatica.
In qualità di membro permanente del CSC, la Divisione Sicurezza prodotto è responsabile della promozione dell'implementazione di tutte le prassi tecniche e gestionali legate alla sicurezza informatica, del coordinamento della costruzione di politiche e procedure di cybersecurity, della conduzione dell'attività, dell'ispezione dell'implementazione della sicurezza, della supervisione e valutazione del progresso della prima linea di difesa.

TERZA LINEA DI DIFESA (DIVISIONE CONTROLLO INTERNO E AUDIT)

La Divisione Controllo interno e audit è la terza linea di difesa per il monitoraggio e la valutazione della governance della cybersecurity. La Divisione Controllo interno e audit è responsabile del controllo della prima e della seconda linea di difesa, compresi i test di conformità e di sicurezza informatica dell'attuazione della procedura, e riferisce i risultati dell'audit al Consiglio di amministrazione/Comitato di revisione. La Divisione Controllo interno e audit può verificare congiuntamente l'implementazione della sicurezza informatica di ZTE con revisori esterni di terze parti. La governance della sicurezza informatica coinvolge anche altri gruppi di supporto, quali risorse umane, finanza e contabilità, strategia e investimenti, gestione delle operazioni, affari pubblici, legali e conformità, affari amministrativi e immobiliari.

SISTEMA DELLE SPECIFICHE DI CYBERSECURITY

ZTE ha stabilito solide politiche, standard, procedure e linee guida sulla sicurezza informatica. Il sistema relativo alla politica in materia di sicurezza informatica raccomanda una serie completa di requisiti per la governance della cyber-security. ZTE ha emesso una serie di specifiche e standard di gestione della sicurezza, che sono sottoposti a revisione periodica. Ogni business unit svolge le attività di sicurezza pratiche in conformità con questi requisiti di sicurezza informatica. Durante l'implementazione pratica delle specifiche di sicurezza, vengono acquisiti i risultati e i registri corrispondenti, che sono disponibili come prova per le parti interessate per l'audit.

IL SISTEMA DI DOCUMENTI PER LA SICUREZZA INFORMATICA ZTE È DIVISO IN QUATTRO LIVELLI:

Primo livello

POLITICA GENERALE DI CYBER SECURITY

Delinea la politica di sicurezza informatica di ZTE. Include l'implementazione tattica, gli obiettivi di sicurezza, i requisiti operativi, le organizzazioni rilevanti e le politiche, le procedure e i documenti essenziali della strategia di sicurezza informatica di ZTE. Tutti i documenti sottostanti sono basati su questo sistema di politica in materia di sicurezza informatica, che comprende: la politica generale di governance, la politica di sicurezza della supply chain, la politica di sicurezza R&S, la politica di sicurezza della consegna, la politica di risposta agli incidenti di sicurezza e la politica di audit della sicurezza.

Secondo livello

SPECIFICHE E PROCEDURE DI GESTIONE DELLA SICUREZZA INFORMATICA

I regolamenti e le procedure che supportano il funzionamento delle politiche di sicurezza. È inclusa una serie di specifiche e procedure di sicurezza dalla supply chain a R&S, consegna e risposta agli incidenti, come specifiche di sicurezza R&S, specifiche di gestione della sicurezza della supply chain, specifiche di gestione della sicurezza della rete e consegna tecnica del servizio di ingegneria, procedura di risposta agli incidenti di sicurezza informatica, standard di codifica sicuri, ecc.

Terzo livello

LINEE GUIDA SULLA SICUREZZA INFORMATICA

I documenti che supportano i regolamenti e le procedure, come la linea guida per gli utenti del tool di sicurezza, le linee guida sulla preparazione della linea di base della sicurezza e le linee guida sul rafforzamento della sicurezza.

Quarto livello

REGISTRI DI SICUREZZA INFORMATICA

I registri dei processi e dei risultati dell'implementazione, come i report di scansione del codice sorgente, i report di valutazione della sicurezza, i registri di analisi delle vulnerabilità e i report di revisione degli incidenti di sicurezza.

SICUREZZA R&S

La sicurezza è una delle massime priorità nelle attività di erogazione del servizio e R&S dei prodotti ZTE. Perseguendo un'efficiente ricerca e sviluppo, ZTE presta un'attenzione significativa alla sicurezza del prodotto e incorpora la "sicurezza" nel ciclo di vita dello sviluppo del prodotto come attributo di base del prodotto, assicurando che ZTE offra funzionalità di erogazione della sicurezza del prodotto affidabili su cui i clienti possono fare affidamento, fornendo ai clienti prodotti e soluzioni sicuri.

PROCEDURE E ORGANIZZAZIONI DI SICUREZZA R&S

Il processo di sviluppo del prodotto ad alte prestazioni (HPPD) è una procedura comune che guida la ricerca e lo sviluppo all'interno di ZTE. Il processo è soggetto a continui miglioramenti ed è regolarmente modificato per soddisfare le esigenze dei clienti e le condizioni del mercato. La sicurezza è un elemento basilare del processo di sviluppo del prodotto ed è integrata nel processo HPPD,garantendo così che la sicurezza sia sviluppata in tutti i nostri prodotti, anche nella fase iniziale della progettazione.

POLITICHE E OBBIETTIVI DI SICUREZZA

Incorporare le attività di sicurezza nella procedura principale di HPPD, integrare i requisiti di gestione della sicurezza nel sistema di revisione e decisionale e assicurare che le politiche e gli obiettivi di sicurezza di ZTE siano implementati nella procedura di R&S prodotto.

Migliorare continuamente le funzionalità di sicurezza, fornire garanzie organizzative per le attività di sicurezza, supportare le procedure di R&S di HPPD e identificare le opportunità per migliorare le attività di sicurezza attraverso metriche di sicurezza e audit di sicurezza.

ZTE combina attività di R&S con riferimento a modelli di pratiche di sicurezza del settore come BSIMM[3] e Microsoft SDL[4] per definire attività di sicurezza quali requisiti di sicurezza, pianificazione della sicurezza, sviluppo della sicurezza, collaudo della sicurezza, consegna e manutenzione della sicurezza nel processo HPPD, per garantire che le funzionalità di sicurezza siano effettivamente integrate nei nostri prodotti. Allo stesso tempo, ZTE migliora continuamente le proprie capacità di sicurezza e fornisce una garanzia organizzativa per le attività di sicurezza, supportando così in modo efficace il funzionamento del processo HPPD. ZTE implementa anche audit della sicurezza e metriche di sicurezza per migliorare continuamente il processo HPPD.

Il processo HPPD è integrato nel processo di sviluppo prodotto con elementi di sicurezza completi al fine di garantire l'effettiva implementazione delle attività di sicurezza. Per fornire prodotti e soluzioni più sicuri ai clienti, i requisiti di sicurezza sono integrati nella procedura aziendale end-to-end, come l'analisi delle minacce alla sicurezza nell'analisi dei requisiti, la progettazione dell'architettura di sicurezza nella progettazione del prodotto, la codifica sicura e la scansione per la sicurezza del codice sorgente nello sviluppo del prodotto, il collaudo delle funzionalità di sicurezza e il collaudo della penetrazione nel collaudo del prodotto, la scansione delle vulnerabilità nella versione del prodotto e la garanzia della coerenza della versione, ecc.

In termini di garanzia dell'organizzazione per la sicurezza della R&S del prodotto, ZTE ha creato un Software Security Group (SSG) con i direttori della sicurezza informatica a formare il core team. Il personale principale dei principali team coinvolti nello sviluppo end-to-end di prodotti quali pianificazione, R&S (requisiti, progettazione, sviluppo e collaudo), supply chain, consegna e mercato, utilizzano tutti un modello di minaccia comune per comprendere i requisiti di sicurezza e garantire che i rischi in tutti i campi coinvolti nei prodotti siano pienamente identificati e che i problemi siano risolti rapidamente. Il CSC a livello aziendale prende decisioni sui principali rischi e problemi legati alla sicurezza informatica e autorizza il supervisore SSG a fornire indicazioni di carattere aziendale al direttore della sicurezza informatica.

3 https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html
4 https://www.microsoft.com/en-us/securityengineering/sdl/

FASE CONCETTUALE

Durante la fase di sviluppo concettuale, ZTE integra i requisiti strategici di sicurezza a medio e lungo termine nella pianificazione della roadmap del prodotto, garantendo nel contempo che i ben noti requisiti di sicurezza a breve termine siano incorporati nella roadmap della versione del prodotto. La pianificazione a breve termine include, in genere, la pianificazione, in base agli attuali requisiti di ammissione al mercato (leggi, regolamenti e standard di settore), requisiti di sicurezza del cliente, analisi della concorrenza, attività industriali, esperienza tra pari, protezione di determinate informazioni e requisiti di sicurezza interni.

I requisiti di sicurezza informatica di ZTE sono composti da due parti: una è la linea di base della sicurezza informatica di ZTE, che viene applicata come i requisiti di sicurezza più basilari. La seconda è la valutazione dei rischi degli scenari applicativi dei prodotti nelle reti degli operatori o nelle reti governative e aziendali e l'integrazione delle contromisure pertinenti nei requisiti di sicurezza.

FASE DI PIANIFICAZIONE

Nella fase di pianificazione, ZTE ha sviluppato una specifica di progettazione della sicurezza del prodotto con riferimento alle specifiche di sicurezza e alle migliori prassi del settore, come ITU-T X.805, ISO 15408, 3GPP e IETF. Durante questa fase, il team R&S perfeziona ulteriormente i requisiti di sicurezza e progetta l'architettura di sicurezza e la sicurezza delle funzionalità dei prodotti in base alle specifiche di progettazione della sicurezza informatica.

ZTE analizza i requisiti di sicurezza e le potenziali minacce alla sicurezza del sistema, determina l'architettura della sicurezza e la soluzione di sistema dei prodotti e assicura che la soluzione di sistema soddisfi i requisiti di sicurezza del mercato e dei nostri clienti. Secondo lo standard di ammissione alla sicurezza ZTE, un team di professionisti verificherà la sicurezza dei prodotti e delle soluzioni dei nostri fornitori e valuterà anche la sicurezza dei componenti di terze parti.

ZTE comprende i requisiti di sicurezza attraverso la modellazione delle minacce. Viene utilizzato un insieme di metodi di modellazione delle minacce di sistema per i prodotti di comunicazione denominati SATRC[5] e si basa sulle migliori prassi del settore, quali ITU-T X.805, STRIDE/DREAD Microsoft, Synopsys ARA e altri modelli.

5 SATRC: Sistema, Asset, Minaccia, Rischio, Controllo

Questo modello garantisce che ZTE sia in grado di:

Definire il sistema

Scomponga lo scenario aziendale, stabilisca il modello di architettura della logica di sistema, identifichi il limite di affidabilità e il punto di ingresso e definisca il diagramma di flusso dei dati.

Identifichi gli asset

Hardware, software, dati e servizio.

Rilevi le minacce

Completi il modello e generi la lista degli attacchi.

Valuta i rischi

Valuti le minacce in base ai rischi causati dalle minacce.

Sviluppi le misure di controllo raccomandate

Determinando le contromisure corrispondenti contro le minacce in base al livello dei rischi.

FASE DI SVILUPPO

Nella fase di sviluppo, l'implementazione del codice e il documento di sicurezza sono sviluppati e completati in conformità con i requisiti delle specifiche di codifica sicura, e il codice viene quindi controllato staticamente e scansionato automaticamente.

CONTROLLO DELLA SICUREZZA DEL CODICE E CODIFICA SICURA

Sulla base delle specifiche di codifica sicura autorevoli del settore, come CERT (Computer Emergency Response Team), OWASP (Open Web Application Security Project), CWE (Common Weakness Enumeration) e STIG (Security Technical Implementation Guide), ZTE ha formulato le specifiche di codifica sicura C/C++/Java/Web.
ZTE gestisce anche strumenti di scansione del codice sorgente leader del settore come Klocwork e Coverity.
ZTE rileva e identifica in modo efficace la qualità, l'affidabilità, le vulnerabilità della sicurezza e la manutenibilità dei vari elementi del codice che compongono i prodotti. ZTE implementa anche misure di monitoraggio e gestione efficaci per i problemi rilevati dagli strumenti, come la gestione Kanban dei dati di Klocwork, che monitora i difetti rimanenti nel tempo.

ZTE ha stabilito un meccanismo di ispezione a tre livelli per il controllo del punto di controllo che scansiona il codice sorgente tre volte, vale a dire: autotest individuale, scansione del modulo e scansione del progetto. Il codice prodotto da ZTE non può passare al punto di controllo successivo se l'obiettivo di zero difetti di sicurezza non viene raggiunto come parte del processo HPPD.

FASE DI COLLAUDO

ZTE sviluppa procedure e soluzioni di collaudo della sicurezza, progetta ed esegue casi di test per verificare i moduli delle funzioni di sicurezza, esegue la scansione delle vulnerabilità, la scansione della robustezza del protocollo, i test di penetrazione sui prodotti e completa un'analisi di vulnerabilità del sistema. ZTE stabilisce la soluzione per implementare un rafforzamento della sicurezza dei prodotti e fornisce la prova necessaria per la certificazione di sicurezza informatica.

FASE DI RILASCIO

I prodotti ZTE sono garantiti per il rilascio solo dopo essere stati controllati con più soluzioni software anti-virus mainstream per il raggiungimento dell'obiettivo zero anomalie. Allo stesso tempo, dal rilascio della versione all'utente per la distribuzione, incluso il processo operativo e di manutenzione, viene eseguita tutta la protezione di sicurezza necessaria per garantire la coerenza della versione rilasciata.

La versione software è protetta con strumenti di mascheramento, come la ridenominazione, la crittografia delle stringhe, l'inserimento di codice virtuale e l'offuscamento della logica del codice, che impediscono a un utente malintenzionato di ottenere il codice originale direttamente utilizzando strumenti di reverse engineering, rafforzando in tal modo la protezione di prodotti ZTE.

GOVERNANCE PER LA SICUREZZA DEI COMPONENTI DI TERZE PARTI

ZTE implementa la gestione di tutto il ciclo di vita dei componenti di terzi richiesti, dall'introduzione di tali componenti di terzi alla loro consegna al cliente come parte del prodotto. ZTE integra la valutazione completa dei rischi per la sicurezza, i test della sicurezza e la gestione delle vulnerabilità dei componenti di terze parti nel processo HPPD. Ciò garantisce che una volta scoperta una vulnerabilità della sicurezza durante il ciclo di vita del prodotto, la vulnerabilità venga valutata e venga fornita una soluzione o elusione a PSIRT per risolvere rapidamente tutti i problemi relativi ai componenti di terze parti.

ZTE ha stabilito un'area per conservare tutti i componenti di terze parti e controlla rigorosamente l'utilizzo dei componenti di terze parti. Ciò garantisce che gli sviluppatori possano ottenere componenti solo da fonti certificate e garantisce a livello centrale che i componenti di terze parti siano conformi, sicuri e aggiornati. ZTE utilizza componenti di terze parti come elementi di configurazione nella procedura di gestione della configurazione del software per garantire che l'utilizzo dei componenti possa essere tracciato.

ZTE è entrato a far parte della comunità open source e continua a monitorare le vulnerabilità individuate dalla community, inviando attivamente soluzioni di vulnerabilità della sicurezza. ZTE contribuisce inoltre attivamente alla sicurezza dei componenti open source.

EROGAZIONE DELLA SICUREZZA CONTINUA

L'erogazione della sicurezza continua di DevSecOps (Sicurezza e funzionamento sviluppo) è garantita da un solido sistema di supporto per la gestione della configurazione e da una toolchain DevOps (Sviluppo e funzionamento) integrata nella procedura di sviluppo.

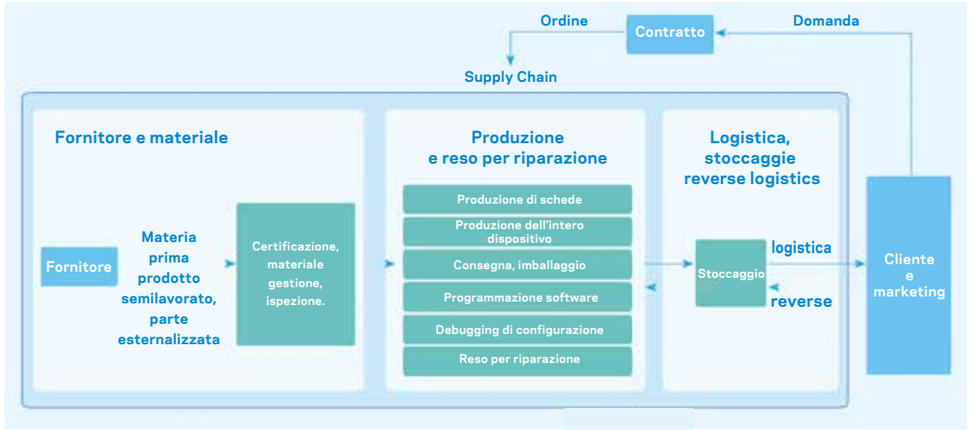
Il sistema di gestione della configurazione di ZTE garantisce la tracciabilità dei requisiti originali del cliente lungo tutte le fasi delle procedure, dalla progettazione, alla codifica del software, al collaudo, all'assicurazione della qualità, all'implementazione della rete esistente e degli errori rilevati sulla rete alla sorgente, dai requisiti originali del cliente al prodotto finale e dal prodotto finale ai requisiti originali - a copertura di tutte le fasi, tutti i processi, tutte le persone coinvolte nel processo di sviluppo software, tutti i componenti e tutti i numeri di versione del software.

Allo stesso tempo, ZTE integra gli strumenti di sicurezza nell'intera toolchain DevOps. Attraverso la pianificazione continua, lo sviluppo collaborativo, i test continui, il rilascio e la distribuzione, i quattro collegamenti sono collegati in serie in modo iterativo. In attività chiave come scansione del codice, test di sicurezza, scansione delle vulnerabilità e protezione della versione, gli strumenti di sicurezza sono garantiti per essere utilizzati in modo efficiente al fine di formare un ciclo chiuso di monitoraggio O&M.

ZTE identifica i rischi per la sicurezza delle informazioni del codice e stabilisce le misure di controllo.
Il personale di R&S accede al cloud desktop attraverso il terminale e accede al cloud R&S.
Il codice è compilato, unità/funzione testata e riesaminata nel cloud R&S per formare la versione da consegnare.
ZTE sviluppa anche una politica di controllo delle risposte per il flusso di codice e documenti tra il cloud desktop e il cloud R&S. Ad esempio, il codice non può essere copiato dal cloud senza approvazione; i soggetti nella whitelist possono accedere a Internet dal cloud desktop, ma non è possibile accedere a Internet dal cloud R&S;
i terminali personali possono accedere a Internet ma non possono accedere al cloud di R&S e alle risorse del servizio IT; lo sviluppo della comunità esterna può essere unito attraverso la libreria dei codici di trasferimento; il controllo regionale di livello A viene eseguito nelle aree di debug per garantire che il codice venga controllato in modo sicuro durante il processo di sviluppo.

SICUREZZA DELLA SUPPLY CHAIN

Con i più alti livelli di apertura in tutto il mondo, il settore delle tecnologie dell'informazione presenta una catena industriale distribuita a livello globale, con fornitori di apparecchiature di comunicazione che richiedono inevitabilmente il supporto di partner commerciali nella catena globale. I componenti di terze parti potrebbero comportare rischi per la sicurezza, ZTE Corporation ha pertanto implementato una serie di misure di monitoraggio nelle operazioni aziendali di gestione materiali e fornitori, produzione e reso per riparazione, logistica e deposito che potrebbero contenere rischi di sicurezza informatica, al fine di garantire che non vengano introdotti, generati o diffusi difetti di sicurezza in queste operazioni e consegnare ai nostri clienti prodotti auto-sviluppati e materiali ausiliari acquistati da terzi sicuri. ZTE integra i requisiti di sicurezza informatica nei processi aziendali della supply chain, compresi il processo di gestione fornitori e materiali, il processo di produzione e reso per la riparazione e i processi di logistica, stoccaggio e reverse logistics.



È stato istituito uno speciale team incaricato dell'assicurazione della sicurezza per identificare eventuali rischi di sicurezza informatica all'interno della supply chain, per perfezionare il processo aziendale ed elaborare efficaci misure di controllo del rischio e schemi di risposta agli incidenti di sicurezza. Inoltre, si stanno apportando costanti miglioramenti per garantire che le misure di controllo della sicurezza informatica siano correttamente implementate e per garantire l'integrità, l'affidabilità e la tracciabilità dei prodotti aziendali lungo tutta la supply chain.

ZTE Corporation ha superato la certificazione ISO 9001 e ha anche aderito al Forum QuEST (Quality Excellence for Suppliers of Telecommunications) e ad oggi è co-presidente per l'Asia-Pacifico e la Grande Cina. Nel 2017, ZTE Corporation è stata ufficialmente certificata ISO28000 (specifica per i sistemi di gestione della sicurezza per la supply chain) e la AEO per la sicurezza doganale, che segna un nuovo traguardo raggiunto dall'azienda in termini di gestione della sicurezza della supply chain.

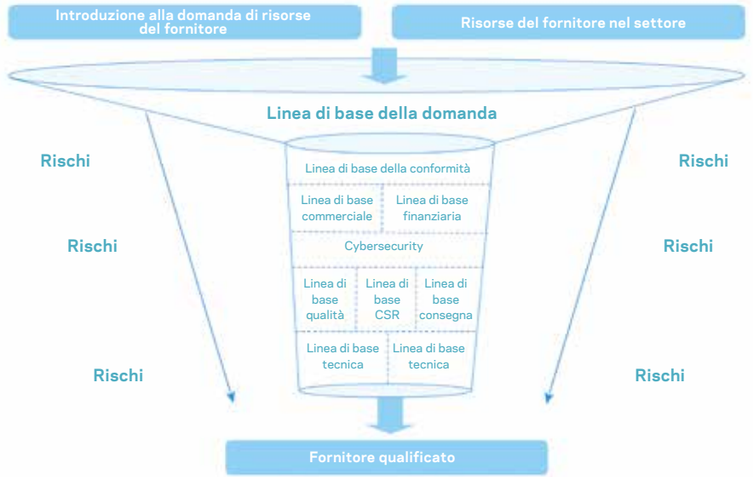
GESTIONE DEI MATERIALI E DEI FORNITORI

ZTE Corporation è impegnata a costruire un rapporto stabile a lungo termine con i nostri partner commerciali. Implementando processi di approvvigionamento strategici e sfruttando costantemente le opportunità di cooperazione con i partner strategici, abbiamo formato un rapporto vincente per entrambe le parti basato su fiducia reciproca, stabilità e sviluppo sostenibile. Nel frattempo ci aspettiamo che i nostri partner commerciali si impegnino in progetti di mercato e R&S dei prodotti per creare più valore.

ZTE ha istituito il forum delle Communities of Practice (COP), che ha consentito un canale completamente nuovo per lo scambio di tecnologie e la comunicazione sulla cybersecurity con i nostri partner commerciali.
È un ambiente di apprendimento in cui l'apprendimento formale e informale è misto.
Fin dalla costituzione del COP di materiali nel 2017, ZTE ha tenuto oltre un centinaio di scambi di tecnologie on-line e off-line con più fornitori. Inoltre, nel 2018 abbiamo ospitato attività CTO Day con numerosi partner commerciali, iniziativa che si è rivelata un grande successo.

L'implementazione di un approvvigionamento strategico non si riflette solo nella collaborazione point-to-point tra ZTE e i singoli fornitori. Siamo altresì impazienti di profondere sforzi congiunti con più partner a monte e a valle per costruire un ecosistema. In questo modo, speriamo di espandere la filiera del settore valorizzando l'innovazione e la pratica su standard, tecnologia, prodotto, mercato e modelli aziendali e di formare un'alleanza strategica più stretta attraverso la pianificazione congiunta, l'integrazione del sistema IT, lo scambio di esperienze manageriali, sfruttando i vantaggi reciproci e apportando miglioramenti insieme attraverso la supply chain.
Nei prosperi settori di 5G, Internet of Things, big data e intelligenza artificiale, continueremo a migliorare la cooperazione con i nostri partner commerciali.

La gestione dei fornitori e dei materiali è una parte fondamentale del sistema di gestione della sicurezza informatica della società. Migliaia di fornitori e partner commerciali dislocati in tutto il mondo, che forniscono in collaborazione decine di migliaia di materie prime, prodotti semilavorati, prodotti finiti o servizi per ZTE, sono una parte fondamentale dei prodotti e delle soluzioni integrate che forniamo ai nostri clienti.



ZTE ha sempre attribuito grande importanza alla creazione di un sistema di gestione dei fornitori e ha stabilito un insieme completo di processi e procedure per la gestione del ciclo di vita dei fornitori, dalla valutazione dell'approvvigionamento, alla certificazione del prodotto, fino alla fornitura al mercato, compresa la gestione della sicurezza informatica, la gestione della responsabilità sociale del fornitore (CSR), la gestione della qualità, la valutazione delle prestazioni e la tracciabilità dei problemi. Un potenziale fornitore può diventare uno dei fornitori qualificati per ZTE, solo dopo aver passato una valutazione completa sulla sicurezza informatica e varie valutazioni in altri ambiti.

In termini di gestione dei materiali, ZTE ha anche sviluppato una serie di procedure di gestione aziendale.
ZTE definisce i rischi di sicurezza informatica dei materiali in tre livelli: alto, medio e basso.
I test di sicurezza informatica dei materiali ad alto rischio vengono condotti quando vengono introdotti nuovi materiali e quando vengono cambiati i materiali vecchi. Per materiali con rischi medi e bassi, chiediamo ai fornitori di condurre una gestione e un controllo autonomo firmando accordi di cybersecurity.
ZTE effettua audit di sicurezza in modo programmato e non sull'implementazione degli accordi da parte dei fornitori.

La risposta del fornitore a un incidente di sicurezza informatica è una parte fondamentale della risposta di ZTE all'incidente di cybersecurity ed ha potenziali effetti sul cliente. ZTE richiede che i fornitori debbano fornire prodotti e servizi in conformità con gli accordi di cybersecurity ed emettere tempestivamente precauzioni e soluzioni alle vulnerabilità, al fine di ridurre al minimo i rischi per la sicurezza dei prodotti esternalizzati. Nel caso in cui vengano rilevate vulnerabilità di sicurezza nel processo di test della sicurezza o utilizzo dei prodotti, i fornitori devono collaborare con ZTE per rintracciare e localizzare il problema e fornire soluzioni con patch software, aggiornamenti, sostituzione o richiamo di materiali difettosi in modo tempestivo.

SICUREZZA DELLA PRODUZIONE E SICUREZZA DEL RESO PER LA RIPARAZIONE

La gestione della cybersecurity durante la produzione è una parte fondamentale del sistema di gestione della sicurezza informatica della nostra azienda. A partire dal sistema di gestione della sicurezza per le specifiche della supply chain, ZTE ha stabilito un sistema di gestione e controllo end-to-end per la sicurezza della produzione, che copre l'intero processo dall'ispezione dei materiali in ingresso, alla produzione dei componenti, all'assemblaggio finale, all'imballaggio del prodotto finito e stoccaggio, compresi una serie di documenti di procedura, linee guida operative e altre istruzioni di lavoro, che integrano i requisiti delle specifiche di sicurezza informatica nelle operazioni di produzione. I requisiti degli standard di sicurezza informatica sono integrati nella formazione e nell'apprendimento della consapevolezza per i dipendenti.

Al fine di controllare i rischi di sicurezza informatica durante la produzione, ZTE ha stabilito un processo di gestione end-to-end per impedire la manomissione di software e hardware, tra cui la sostituzione non autorizzata dell'hardware, l'inserimento o la manomissione del software e l'infezione da virus. Nel processo di produzione, ZTE ha identificato diverse procedure chiave relative alla sicurezza informatica, compresa la gestione della versione del software, la programmazione dei chip, il test finale dell'assemblaggio delle schede di circuito stampato (PCBA), il debug del modulo, le prove di invecchiamento, il debug di tutto il dispositivo, l'imballaggio, il reso per la riparazione, ecc. In base ai livelli di rischio della cybersecurity, ZTE classifica tutte le aree di produzione e stoccaggio in tre diversi livelli di aree di controllo della sicurezza informatica, di cui le aree di livello I e II sono le aree rigorosamente gestite. Gli amministratori della sicurezza sono designati in tutte le aree rigorosamente gestite per implementare la supervisione ordinaria e altre misure di controllo della sicurezza. Inoltre, con la premessa della conformità alle leggi e ai regolamenti applicabili, ZTE conduce anche una normale indagine di background sul personale in posizioni sensibili legate alla sicurezza informatica, per evitare qualsiasi rischio di cybersecurity potenzialmente causato da fattori umani. Nel processo di gestione della sicurezza informatica, gli ingegneri ZTE possono archiviare e rilasciare il software solo attraverso il sistema PDM (Product Data Management) a cui possono accedere, al fine di proteggere il software da manomissioni durante la produzione.

ZTE adotta il Manufacturing Execution System (MES) per registrare informazioni complete sul processo di produzione. Consente un efficace monitoraggio end-to-end delle informazioni sul processo di produzione del prodotto in base al codice a barre del prodotto e alle informazioni sui lotti. È anche possibile rintracciare i numeri di lotto dei materiali in ingresso (numeri di sequenza) dei prodotti e dei componenti del fornitore. Nel frattempo, con l'uso condiviso del sistema di Supply Chain Management (SCM) per l'acquisto e del sistema di Warehousing Management (WMS) per la consegna, il MES consente un processo di monitoraggio e gestione end-to-end dall'acquisto del materiale alla consegna del prodotto. Utilizzando queste misure di gestione, ZTE può localizzare il dispositivo, il pezzo, la scheda o il componente che presenta problemi di qualità o vulnerabilità di sicurezza e ottenere la quantità e lo stato di prodotti disponibili in magazzino, in produzione, in transito o ricevuti dai clienti per migliorare l'efficacia della risposta agli incidenti di sicurezza.

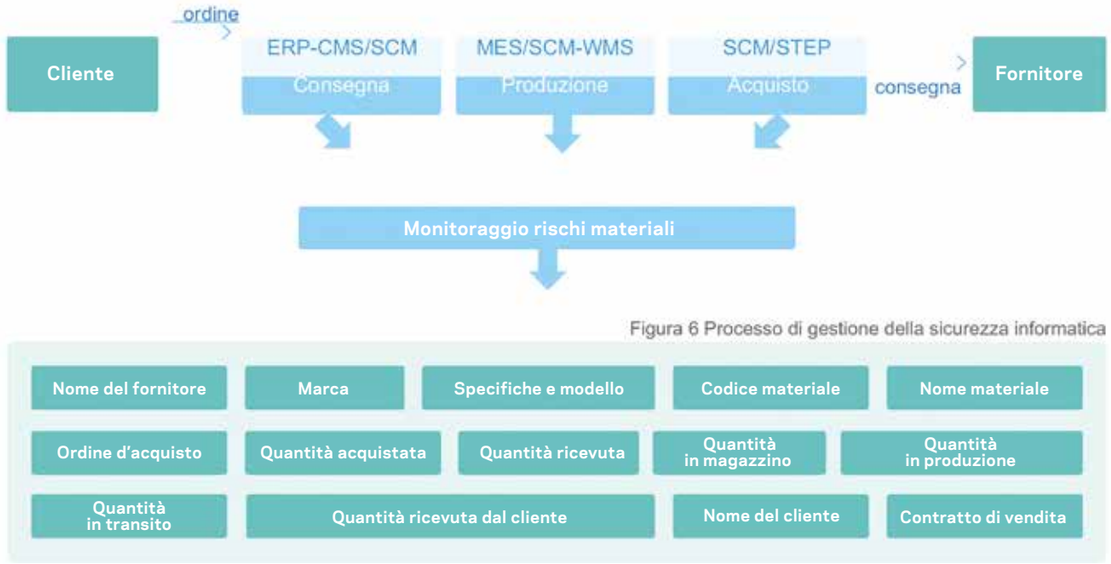


Figura 6 Processo di gestione della sicurezza informatica

La sicurezza informatica nell'operazione di reso per la riparazione è una parte fondamentale della gestione della sicurezza informatica per ZTE. Quando i prodotti difettosi vengono restituiti per la riparazione, ZTE ricorda al cliente l'elaborazione di informazioni sensibili tramite il processo RMA (Return Material Authorization Request) o altrimenti, come l'archiviazione dei dati, l'eliminazione o la rimozione del supporto di archiviazione mobile, prima di restituire gli articoli per la riparazione. Inoltre, dopo aver trasferito l'apparecchiatura a ZTE, garantiremo la protezione della sicurezza dei prodotti software e hardware dell'apparecchiatura.

Nel processo di riparazione, ZTE utilizza solo materiali di fornitori qualificati e certificati. È vietato utilizzare materiali o componenti provenienti da fonti sconosciute, per garantire che l'apparecchiatura restituita per la riparazione non venga compromessa. Le misure corrispondenti vengono prese anche durante il periodo di riciclo dei materiali e dell'apparecchiatura, come la registrazione di video e l'isolamento della rete, per garantire che l'apparecchiatura restituita per la riparazione non venga illegalmente manomessa, colpita da infezioni da virus o violazioni dei dati. ZTE ha processi e requisiti speciali per la cancellazione dei dati nella fase di riparazione. Le apparecchiature oltre la riparazione e la sostituzione saranno raccolte ed elaborate da un'unità speciale. Il reso per la riparazione delle apparecchiature viene gestito sul sistema ECC-ASM dove vengono registrati i dati dell'intero processo di riparazione per scopi di monitoraggio e dove è possibile conoscere lo stato e il responsabile della riparazione. Il sistema ha funzioni complete per la ricerca, la registrazione e l'analisi delle informazioni.

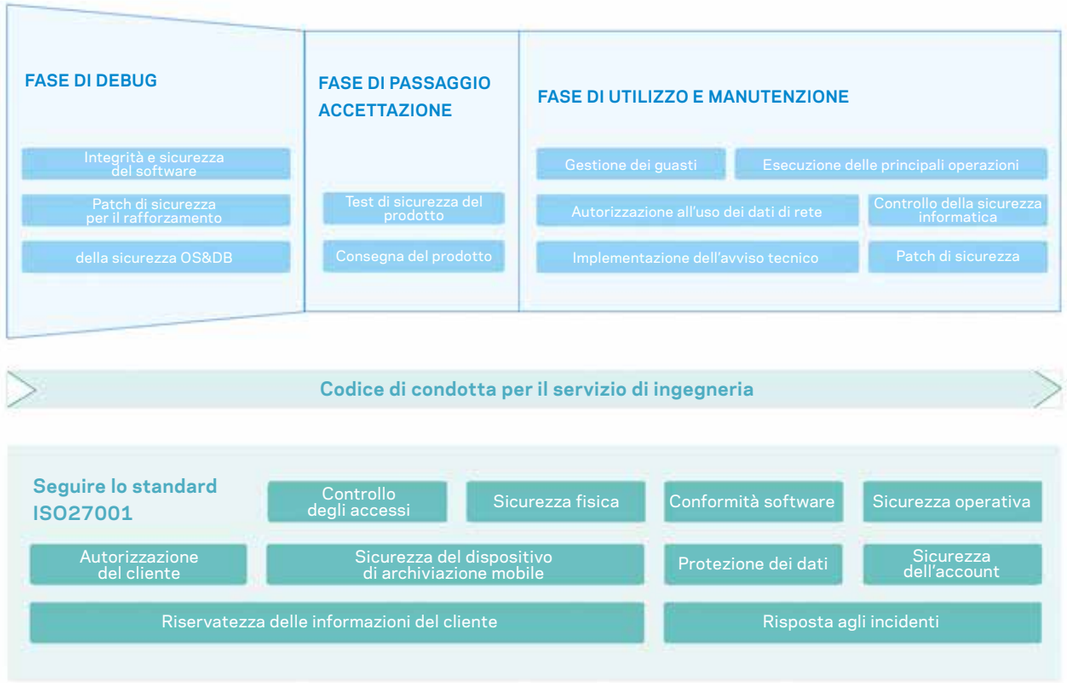
SICUREZZA DI MAGAZZINO E LOGISTICA

In termini di logistica e stoccaggio, in base ai sei centri logistici nazionali e in collaborazione con i fornitori di servizi logistici globali, ZTE sta sviluppando un sistema di centri logistici nazionali, passo dopo passo, migliorando le prestazioni della rete globale della supply chain e pianificando le migliori rotte merci per garantire la consegna tempestiva del progetto. Attraverso sforzi congiunti con fornitori di servizi logistici di livello mondiale altamente qualificati, basati sulla tecnologia IoT e una piattaforma intelligente, ZTE ha implementato la visualizzazione a livello di intero processo dello stato della logistica, garantendo la sicurezza fisica delle merci del cliente. ZTE è in grado di tracciare a livello di intero processo le merci in magazzino attraverso il sistema di Warehousing Management. ZTE aggiorna regolarmente il sistema IT di logistica e stoccaggio, i dispositivi di monitoraggio e le strutture di sicurezza per evitare l'inserimento e la sostituzione illecita di codici o il danneggiamento dei componenti principali durante le procedure di logistica e stoccaggio. La query con un clic delle informazioni sugli ordini e la visualizzazione degli stati a livello di processo sono implementate tramite una piattaforma di visualizzazione.

Il processo completo di gestione della reverse logistics stabilito in ZTE ha reso possibili schemi di reverse logistics in conformità con le leggi e i regolamenti locali dei paesi e delle regioni, per soddisfare i requisiti di sicurezza delle informazioni e protezione della privacy dei clienti e dei paesi e delle regioni locali in cui si trovano i clienti. Nel caso in cui l'apparecchiatura restituita contenesse dati sensibili, ZTE ricorderà e richiederà ai clienti di cancellare i dati prima di restituirla per la riparazione. Se un prodotto deve essere rottamato, deve essere richiesto un rapporto di distruzione al distributore di riciclaggio. I prodotti sensibili dovrebbero essere smaltiti sotto la supervisione in loco da parte di personale appositamente incaricato.

CONSEGNA DI SICUREZZA

Proteggere la sicurezza dei prodotti consegnati ai nostri clienti è il nostro obiettivo nella consegna.
ZTE utilizza sia misure tecniche che gestionali per garantire la consegna sicura: Da un lato, prodotti e servizi sicuri vengono consegnati ai clienti come previsto. Dall'altro, tutto il personale in loco è tenuto a seguire i codici di condotta relativi alla consegna.



Un ciclo di consegna del progetto completo copre tre fasi: debug, passaggio/accettazione e utilizzo e manutenzione. I punti chiave di controllo della sicurezza sono impostati in ciascuna fase. In base alle caratteristiche del servizio n ciascuna fase, vengono definite delle misure di sicurezza nel campo delle consegne per ridurre i possibili rischi causati da operazioni non standard. I potenziali rischi per la sicurezza sono scoperti ed eliminati in modo tempestivo utilizzando flussi di sicurezza, regolamenti e metodi verificabili e ripetibili in conformità con standard coerenti di sicurezza informatica. ZTE ha formulato i codici di condotta per il settore delle consegne secondo le leggi e i regolamenti globali, i requisiti del cliente e le migliori prassi (ad esempio, lo standard ISO27001), per garantire la sicurezza dei prodotti e dei servizi forniti ai nostri clienti.

TRE FASI DI SICUREZZA DELLA CONSEGNA

FASE DI DEBUG

Nella fase di debug, le misure di verifica sono rigorosamente implementate nel campo di consegna dei prodotti per impedire la modifica accidentale della configurazione. Il software viene scaricato solo da un sito Web specificato. Inoltre, i controlli di coerenza del software devono essere eseguiti prima dell'installazione per garantire l'integrità del software. Durante il periodo di messa in servizio e debug, il personale in loco intraprende una serie di azioni come il rilevamento di programmi dannosi attraverso misure tecniche, l'installazione di sistemi operativi designati o patch di database, la scansione delle vulnerabilità e il completamento delle configurazioni di miglioramento in conformità con le linee guida in materia di configurazione della conformità prodotto e rafforzamento della sicurezza prodotto.

FASE DI PASSAGGIO/ACCETTAZIONE

Prima della consegna di un progetto, vengono eseguiti alcuni test di sicurezza (con le configurazioni temporanee rimosse) per garantire la sicurezza dei prodotti e vengono emessi i rapporti di prova.
I prodotti possono essere consegnati ai clienti solo dopo aver superato la procedura di accettazione.
Oltre alle attrezzature fisiche, le merci ufficialmente consegnate ai clienti includono anche rapporti di prova completi e documenti. Sarà inoltre garantita la sicurezza degli account e delle password di sistema.

FASE DI UTILIZZO E MANUTENZIONE

I rischi per la sicurezza variano a seconda delle minacce nuove ed emergenti, delle leggi e dei regolamenti, dei modelli di attacco e delle vulnerabilità, il personale addetto alle consegne di ZTE monitora continuamente i cambiamenti nella fase di utilizzo e manutenzione per impedire la divulgazione e la manomissione dei dati nel processo di reso per la riparazione, conducendo regolari controlli di sicurezza e installando patch di vulnerabilità senza indugio alcuno. Tutte le operazioni sono autorizzate dai clienti.

GESTIONE DEI SUBAPPALTATORI

Qualsiasi comportamento non sicuro dei subappaltatori nel processo di consegna potrebbe incrementare i rischi di consegna. Il controllo della sicurezza è implementato nel campo delle consegne da tre prospettive: gestione, capacità e supervisione.

IN TERMINI DI GESTIONE

ZTE formula innanzitutto adeguati regolamenti di sicurezza in base alle leggi e ai regolamenti locali e alle politiche di sicurezza. Nel frattempo i subappaltatori sono tenuti a firmare un contratto di leasing integrato con responsabilità e obblighi di sicurezza. Inoltre, con la premessa della conformità alle leggi e ai regolamenti applicabili, ZTE effettua indagini preliminari di background sui potenziali subappaltatori e valutazioni dei rischi correlati alle posizioni per le quali i subappaltatori si candidano.

IN TERMINI DI CAPACITÁ

I subappaltatori dovranno firmare una lettera di impegno prima di poter accettare qualsiasi lavoro.
Verranno condotti dei programmi di formazione per migliorare la consapevolezza della sicurezza e le competenze di sicurezza. I subappaltatori possono lavorare per i team di progetto solo dopo aver superato la valutazione delle capacità.

I TERMINI DI SUPERVISIONE

I computer dei subappaltatori saranno sottoposti a un controllo di sicurezza prima che i subappaltatori entrino a far parte ufficialmente del team di progetto. Le azioni correttive devono essere richieste per il computer che non supera l'audit fino a quando non soddisfa i requisiti di sicurezza.
Controlli regolari sulla sicurezza dei computer dei subappaltatori sono implementati per assicurarsi che non sia installato alcun software dannoso o non autorizzato.
Dopo la risoluzione del contratto con ZTE e prima di lasciare il team di progetto, i subappaltatori saranno tenuti a cancellare tutti i dati relativi alla società, ai clienti e ai servizi sui loro computer.
L'uscita è consentita solo dopo aver superato il controllo di sicurezza.

SICUREZZA DELLE INFORMAZIONI

La sicurezza delle informazioni viene utilizzata per proteggere la sicurezza degli asset dell'azienda in modo che R&S, produzione e operazioni del prodotto possano essere eseguite in un ambiente sicuro.
Stabilendo un sistema completo di gestione della sicurezza delle informazioni, è possibile definire misure di controllo in termini di organizzazione, personale, procedure e tecnologia per garantire la riservatezza, l'integrità e la disponibilità di dati e asset, il miglioramento dei livelli di sicurezza delle informazioni e la salvaguardia dello sviluppo della società.

ZTE ha istituito un sistema di gestione della sicurezza delle informazioni (ISMS) in cui sono definiti i processi di gestione della politica generale di sicurezza delle informazioni, la politica di sicurezza, la classificazione delle informazioni, la valutazione del rischio e la verifica della sicurezza ed è supportata da red line di sicurezza delle informazioni. L'organizzazione per la sicurezza delle informazioni monitorerà le red line per supervisionare, investigare e affrontare eventuali violazioni della sicurezza delle informazioni aziendali e violazioni dei segreti commerciali della società. Ogni anno, tutti i dipendenti riceveranno formazione sulla sicurezza e saranno sottoposti a test per incrementare e mantenere la consapevolezza della sicurezza. La società ha costruito diversi canali di segnalazione per la sicurezza. Ad esempio, quando si tratta di violazioni della sicurezza delle informazioni ed eccezioni, come l'esposizione al rischio e alla vulnerabilità, i dipendenti possono segnalarle tramite i seguenti canali, e-mail, telefono e il sito Web ufficiale della società, oltre a essere incoraggiati a gestire le eccezioni, risolvere le vulnerabilità e completare le regole di sicurezza in modo tempestivo.

ZTE ha adottato una serie di iniziative in materia di classificazione delle informazioni, sicurezza del personale, sicurezza fisica e sicurezza IT per garantire la sicurezza degli asset della società e garantire la riservatezza, l'integrità e la disponibilità degli asset, migliorando al tempo stesso il livello di sicurezza delle informazioni come competenza chiave della società.

CLASSIFICA DELLE INFORMAZIONI

ZTE ha classificato l'importanza delle informazioni aziendali in quattro livelli:

Top secret: si riferisce alle informazioni top secret, una violazione causerà un danno significativo agli interessi aziendali.

Riservato: si riferisce alle informazioni molto riservate, una violazione causerà un danno molto significativo agli interessi aziendali.

Confidenziale: si riferisce alle informazioni riservate, una violazione causerà un danno significativo agli interessi aziendali.

Solo per uso interno: si riferisce alle informazioni che tutti i dipendenti devono conoscere, ma non adatte lla divulgazione al pubblico.

ZTE ha anche formulato misure di controllo corrispondenti per ogni livello di informazione.
ZTE protegge le informazioni dei clienti classificando i loro dati in modo simile, con la maggior parte delle informazioni dei clienti classificate nel livello riservato o confidenziale.

SICUREZZA DEL PERSONALE

La sicurezza del personale è di pari importanza in quanto la consapevolezza della sicurezza e il comportamento dei dipendenti svolgono un ruolo vitale in una sequenza di attività end-to-end come R&S, produzione e consegna dei prodotti. ZTE mantiene una politica di controllo sulla sicurezza del personale durante l'intero ciclo di vita del prodotto. Per una posizione personale a un livello speciale, con riserva della conformità alle leggi e ai regolamenti applicabili, ZTE affiderà a una società di terze parti l'esecuzione di verifiche di background e indagini sul candidato. Esistono clausole di riservatezza contrattuale stipulate in un contratto di lavoro ZTE, che informano i dipendenti sull'adempimento delle loro mansioni in modo confidenziale e responsabile. I dipendenti sono inoltre tenuti a seguire corsi di formazione sulla sicurezza durante l'inserimento del personale. Durante il loro impiego, i dipendenti devono firmare l'impegno alla sicurezza delle informazioni di ZTE e riceveranno una formazione sulla sicurezza delle informazioni e dovranno sostenere un esame almeno una volta all'anno. Quando i dipendenti si dimettono, sono tenuti a firmare la Dichiarazione sulla sicurezza delle informazioni per la dimissione dei dipendenti e si impegnano a non prelevare alcuna informazione aziendale. Nel frattempo, i dipendenti, a seconda delle posizioni ricoperte, devono essere svincolati da informazioni segrete o rispettare l'Accordo di non concorrenza.

SICUREZZA FISICA

A seconda del livello di segretezza in cui una divisione di una regione è classificata, ZTE ha fisicamente suddiviso i livelli di sicurezza delle aree in base al seguente schema di classificazione, area segreta fondamentale di livello A,area segreta importante livello B, area segreta generale di livello C area e area pubblica di livello D.
Quando i dipendenti entrano in azienda, devono presentare l'ID personale per l'autenticazione.
Qualsiasi visita alla società deve essere documentata dal receptionist prima dell'arrivo del visitatore.
Il personale di sicurezza può consentire l'accesso a un visitatore solo dopo aver verificato la sua identità.
Le aree principali della società definite a livello A o B sono dotate di controlli fisici a parte, come i sistemi di controllo dell'accesso delle porte, un cancello di sicurezza o il personale addetto alla sicurezza. In tutta la regione vengono effettuati controlli e pattugliamenti 24 ore su 24, 7 giorni su 7, e vengono installati monitor per una maggiore sicurezza. Ad esempio, l'area di debug di R&S e il laboratorio di sicurezza sono gestiti utilizzando controlli di livello A per garantire che la sicurezza del codice venga mantenuta durante lo sviluppo. Inoltre, per un'efficace prevenzione e ispezione sulla sicurezza delle informazioni, sono state implementate diverse misure tecniche di controllo, ad esempio, l'installazione di controlli di accesso alle porte e monitor nelle aree chiave e il divieto di copiare e fotografare.

SICUREZZA IT

Il supporto IT è fondamentale per l'efficace gestione delle attività aziendali all'interno della società in quanto il sistema IT contiene una grande quantità di informazioni riservate. Una serie di attività relative a R&S, supply chain e fornitura dei processi e delle procedure aziendali è supportata e protetta dal sistema IT. In questo modo, i registri possono essere controllati e tracciati con non rifiuto.

Il cloud desktop ZTE e il cloud R&S sono costruiti e standardizzati per l'utilizzo nei principali campi di protezione della sicurezza, come nei laboratori di R&S. Tutta l'attività di R&S è sviluppata nel cloud, assicurando che il codice relativo al prodotto e i documenti chiave siano archiviati in modo sicuro nella piattaforma cloud.
È vietato copiare e inviare informazioni al di fuori della società senza autorizzazione. Inoltre, l'accesso a Internet non è disponibile per il cloud desktop e il cloud R&S nelle aree protette. Allo stesso tempo, l'autorizzazione dell'accesso Internet al desktop cloud è disabilitata di default. I desktop Cloud di utenti diversi sono separati in termini di memoria e dati. Il server di gestione dei codici è accessibile solo attraverso l'ambiente cloud desktop per il personale di R&S.

La Divisione di gestione delle informazioni dell'azienda verifica regolarmente le reti in relazione ai principali sistemi, server e database degli uffici e invia suggerimenti a unità e persone responsabili, esortandoli a rettificare eventuali problemi o chiarire eventuali dubbi entro un determinato periodo.

GESTIONE DEGLI ASSETS

La gestione degli asset è la base della sicurezza delle informazioni e qualsiasi vulnerabilità, intrusione o violazione deve essere individuata e gestita in base agli asset. Dal punto di vista della sicurezza delle informazioni, gli asset si riferiscono a tutto ciò che è prezioso per l'azienda, inclusi l'area fisica, il personale, i documenti elettronici o cartacei, i database, il software, l'hardware, i dispositivi mobili, le applicazioni e altri supporti di informazioni o informazioni. Pertanto, abbiamo classificato gli asset per monitorare e confermare le informazioni di configurazione accurate degli asset ZTE.
Le responsabilità devono essere definite per il personale in modo da poter condurre una gestione durante tutto il ciclo di vita degli asset.

Tutto l'hardware, come il server e i computer dell'azienda, ha un numero di asset fisso e un'etichetta.
L'amministratore di un asset fisso di una divisione è responsabile della gestione e del controllo degli asset.
Se gli asset hardware come i computer vengono portati fuori dall'area dell'ufficio, devono essere registrati nel sistema e inoltrati preventivamente ai responsabili competenti affinché l'autorizzazione venga concessa.
Il personale addetto alla sicurezza dovrebbe eseguire la scansione, identificare e confermare le etichette degli asset.

ID AUTENTICAZIONE E PERMESSO

Il principio della gestione dell'autenticazione dell'identità e dell'autorizzazione minima è stato applicato alla protezione IT sulla sicurezza delle informazioni. Ad esempio, dopo l'iscrizione, ogni dipendente dispone solo dei permessi di base e necessari per i sistemi di finanza, personale e IT, mentre altri permessi speciali devono essere richiesti sul sito Web IT. Nella richiesta occorre specificare le ragioni (requisiti di lavoro) e il periodo di autorizzazione. Dopo essere stato autorizzato da un responsabile, una persona di supporto IT dedicata elabora e configura l'autorizzazione in base al ruolo della persona.
La Divisione gestione delle informazioni verifica periodicamente le autorizzazioni dei sistemi IT dei dipendenti.

Esistono misure di protezione della sicurezza implementate in vari modi per autenticare l'identità di un utente. Innanzitutto, quando si accede al sistema aziendale tramite la password dell'account, viene eseguita l'autenticazione a doppio fattore. In secondo luogo, viene applicato un metodo di password complessa nell'impostazione della password dell'account. In terzo luogo, se la password viene inserita in modo errato per un determinato numero di tentativi, l'account si blocca. In quarto luogo, se il dispositivo viene perso, l'approvazione sarà richiesta nel sistema IT prima di vincolare i dati a un altro dispositivo

Inoltre, alcune autorizzazioni di sistema sono valide in determinati periodi e verranno revocate automaticamente alla scadenza. Quando le autorizzazioni all'account applicate dai dipendenti scadono o falliscono, come il permesso di accesso alla VPN (Virtual Private Network) e l'autorizzazione alla posta in uscita, vengono automaticamente revocate dal sistema. L'utente deve richiederle se è necessario ripristinare le autorizzazioni. Quando un dipendente si dimette o cambia mansione, le autorizzazioni corrispondenti iniziali verranno annullate. ZTE gestisce i rischi per la sicurezza ai massimi livelli grazie al controllo coerente del nostro sistema IT.

SICUREZZA DELLA RETE

ZTE ha implementato misure di sicurezza rilevanti per controllare la rete dell'infrastruttura in termini di sicurezza dell'accesso alla rete, sicurezza delle operazioni a distanza e della manutenzione e sicurezza della configurazione. La società fornisce un ambiente di rete sicuro per R&S, produzione e servizi operativi attraverso misure quali il controllo degli accessi, la segregazione della sicurezza e la protezione dei confini.

I dispositivi collegati alla rete aziendale devono soddisfare i requisiti di sicurezza di base e superare un'autenticazione dell'identità utente. Prima di autorizzare una connessione, il sistema eseguirà automaticamente più controlli di sicurezza sui terminali. Solo i terminali qualificati ottengono l'accesso alla rete ZTE, dove sono installati il software di sicurezza desktop e il software di sicurezza dei documenti della società, le patch di sicurezza vengono installate automaticamente, il software antivirus viene regolarmente aggiornato e il software ad alto rischio e il software con rischio di proprietà intellettuale non sono installati.

Abbiamo implementato la segregazione di rete per gestire le minacce alla sicurezza interne sulla rete. Ad esempio, la rete R&S e la rete aziendale sono reti isolate e la rete di produzione e la rete aziendale sono isolate.

Ai limiti della rete, vengono utilizzati firewall, rilevamento e protezione dalle intrusioni e altri strumenti di rilevamento automatico. Sotto il rigoroso monitoraggio di questi strumenti, le minacce alla sicurezza esterne alla rete vengono notevolmente ridotte e viene creato un ambiente di rete sicuro per R&S, produzione e lavoro d'ufficio in azienda.

PROTEZIONE DEI DATI PERSONALI

Sullo sfondo del rapido sviluppo della rete di comunicazione, big data e cloud computing, sempre più dati personali vengono raccolti, archiviati, trasmessi e utilizzati in tutte le reti. Al fine di proteggere la sicurezza di questi importanti dati personali, i principali paesi e regioni hanno promulgato una serie di leggi e regolamenti nel campo della protezione dei dati, come il regolamento generale sulla protezione dei dati (GDRP) dell'Unione europea (UE), il California Consumer Privacy Act del 2018 degli Stati Uniti e la Cybersecurity Law della Cina. Per ZTE, la protezione dei dati non è solo un requisito legale, ma anche un'importante garanzia per la governance della conformità aziendale e la gestione della sicurezza.

Integrando la protezione dei dati nel sistema di conformità aziendale, ZTE ha promosso la protezione dei dati personali e e garantito la sicurezza dei dati concentrandosi sugli scenari principali, migliorando le organizzazioni, introducendo misure tecniche e ottimizzando i metodi di gestione. Inoltre, ZTE considera la protezione dei dati come un impegno personale per la sicurezza informatica. Pertanto, l'azienda ha integrato il concetto di protezione dei dati nella progettazione del prodotto e nel processo di erogazione del servizio, soddisfacendo continuamente l'attuale requisito imposto dai regolamenti sulla protezione dei dati globali e andando oltre tali regolamenti.
ZTE intende raggiungere una strategia di sviluppo sostenibile insieme ai nostri clienti globali, fornitori e altri partner, strategia che sia sicura e affidabile.

SISTEMA DI CONFORMITÀ DELLA PROTEZIONE DEI DATI

A seconda del livello di segretezza in cui una divisione di una regione è classificata, ZTE ha fisicamente suddiviso i livelli di sicurezza delle aree in base al seguente schema di classificazione, area segreta fondamentale di livello A area segreta importante livello B, area segreta generale di livello C area e area pubblica di livello D. Quando i dipendenti entrano in azienda, devono presentare l'ID personale per l'autenticazione. Qualsiasi visita alla società deve essere documentata dal receptionist prima dell'arrivo del visitatore. Il personale di sicurezza può consentire l'accesso a un visitatore solo dopo aver verificato la sua identità. Le aree principali della società definite a livello A o B sono dotate di controlli fisici a parte, come i sistemi di controllo dell'accesso delle porte, un cancello di sicurezza o il personale addetto alla sicurezza. In tutta la regione vengono effettuati controlli e pattugliamenti 24 ore su 24, 7 giorni su 7, e vengono installati monitor per una maggiore sicurezza. Ad esempio, l'area di debug di R&S e il laboratorio di sicurezza sono gestiti utilizzando controlli di livello A per garantire che la sicurezza del codice venga mantenuta durante lo sviluppo. Inoltre, per un'efficace prevenzione e ispezione sulla sicurezza delle informazioni, sono state implementate diverse misure tecniche di controllo, ad esempio, l'installazione di controlli di accesso alle porte e monitor nelle aree chiave e il divieto di copiare e fotografare.

ZTE ha eseguito una serie di miglioramenti specifici nella protezione dei dati in termini di organizzazione, regole, accordi, formazione e tecnologia. In termini di sistema organizzativo, è stata stabilita una modalità di "supporto da parte di un team di professionisti, a tre linee di difesa per il controllo e la collaborazione tra più entità interne ed esterne". ZTE ha inoltre creato una struttura di regole su quattro livelli, "Politica, regolamento generale, linee guida di servizio, accordi e registri", per aiutare le divisioni a identificare e rispondere ai rischi di protezione dei dati nelle attività aziendali in base ai rispettivi scenari di gestione. Il sistema di accordi funge da base fondamentale per la conformità dei dati, consentendoci di organizzare e promuovere la firma di accordi legalmente vincolanti in modo unificato.

Per quanto riguarda il sistema di formazione, viene istituito un meccanismo integrato di sviluppo del corso, implementazione della formazione e supervisione degli effetti per sensibilizzare e incrementare le capacità di un dipendente in materia di rispetto della protezione dei dati da più punti di vista. Nel sistema tecnologico, abbiamo attivamente adottato e continuato a cercare il miglior approccio tecnico applicabile per la protezione dei dati. Inoltre, i requisiti di conformità vengono eseguiti con l'aggiornamento del sistema delle informazioni e strumenti professionali. In un sistema commerciale, ci affidiamo a uno speciale servizio di consulenza sulla conformità per eseguire la difesa e il controllo del rischio nei processi commerciali come le fiere e gli eventi di grandi dimensioni.

Pertanto, attraverso sforzi sistemici, ZTE ha stabilito linee guida e standard di conformità alla protezione dei dati che regolano il nostro core business che aiuta le unità funzionali e tutti i dipendenti nelle loro posizioni a comprendere i nostri principi di protezione dei dati e a seguire rigorosamente le normative e le procedure applicabili della società. ZTE ha inoltre firmato il Contratto di elaborazione dei dati (DPA), la clausola contrattuale standard (SCC, trasferimento dati oltreconfine), integrata dalla lettera di notifica e dalla lettera di autorizzazione che sono coerenti con i requisiti GDPR. Inoltre, abbiamo applicato tecnologie di sicurezza tramite crittografia, anonimato e pseudonimi e adottato misure di sicurezza quali l'autenticazione a doppio fattore, la gestione delle autorizzazioni e il monitoraggio degli accessi, che supporteranno la protezione dei dati e la difesa della sicurezza nei processi di raccolta, archiviazione, uso, trasferimento e distruzione

MECCANISMO DI RISPOSTA DELLA PROTEZIONE ALLA VIOLAZIONE DEI DATI

La risposta alla violazione dei dati ha ricevuto la massima attenzione nell'intero sistema di conformità nella protezione dei dati. Di conseguenza, ZTE ha creato un meccanismo per la risposta agli incidenti di violazione dei dati con una rapida collaborazione tra più parti al centro di tale meccanismo. Abbiamo specificato le procedure di risposta e sviluppato un sistema di risposta. L'operazione specifica è supportata dal team responsabile della protezione dei dati che copre ampiamente tutte le linee aziendali e le regioni, nonché il team di specialisti e il team del Data Protection Officer. In caso di un incidente sospetto, elaborano e organizzano rapidamente le risposte, proteggono i dati personali in conformità con le regole, riducono le potenziali perdite e conducono il processo di notifica. Nel frattempo, l'intero processo di risposta agli incidenti verrà registrato nell'apposito sistema di segnalazione, per preparare l'eventuale riferimento del documento e la presentazione delle prove all'agenzia di regolamentazione. ZTE organizza di volta in volta esercitazioni di risposta agli incidenti su violazioni dei dati e rafforza l'efficacia del meccanismo di responsabilità agli incidenti e di responsabilità quotidiana per prevenire violazioni dei dati e gestire le violazioni dei dati in modo organizzato.

Per garantire l'attuazione di ogni politica e iniziativa, ZTE ha costruito un meccanismo di controllo della protezione dei dati e ha attivato canali per la segnalazione delle violazioni. In particolare, ZTE ha sviluppato un team di audit della conformità a tempo pieno e incorporato l'autocontrollo e l'audit nel meccanismo di controllo interno e garantisce che il meccanismo svolga la supervisione di routine e promuove un ciclo positivo che coinvolge la sensibilizzazione, l'investimento di risorse, la ricostruzione delle procedure e il miglioramento delle capacità in materia di protezione dei dati.

PRATICA DELLA SOLUZIONE DI PROTEZIONE DEI DATI

In base a soluzioni tecniche innovative, ZTE ha praticato e integrato i requisiti di protezione dei dati personali con i requisiti di sicurezza informatica e ha sperimentato un sistema di soluzioni e sistemi di prodotto sicuro e conforme.

Abbiamo utilizzato metodi e pratiche di protezione dei dati personali durante il ciclo di vita del prodotto per aumentare il livello di conformità della protezione dei dati. Conformemente ai principi di privacy di default e privacy di design, ZTE mantiene il senso del controllo della sicurezza nella fase di progettazione del prodotto aderendo alle Specifiche di valutazione dell'impatto sulla protezione dei dati generali e alla Valutazione dell'impatto sulla protezione dei dati di progettazione del prodotto. La protezione dei dati personali e l'elaborazione della tecnologia di sicurezza sono considerati come gli attributi predefiniti di cybersecurity per garantire che l'elaborazione dei dati personali avvenga in modo legale, equo e trasparente.

Sulla base di un progetto di protezione tramite mascheramento dei dati di prodotto autorizzato dal cliente, il responsabile del trattamento e l'incaricato al trattamento dei dati possono interagire tra loro per garantire la sicurezza dei servizi di più parti attraverso l'uso del centro di autorizzazione, della rete di sicurezza, della mascheratura degli elementi di rete e dei progetti di tecnologia della sicurezza. In caso di accesso a distanza alla soluzione dei problemi tecnici e alla gestione delle risposte agli incidenti dei clienti nella regione UE, viene adottata una soluzione di accesso a distanza in modalità sicurezza basata sul Contratto di trasferimento dei dati oltreconfine, in modo da cooperare con il cliente, gli ingegneri locali dell'UE e gli ingegneri presso la nostra sede centrale in Cina, e svolgere pratiche di protezione dei dati auto-guidate.

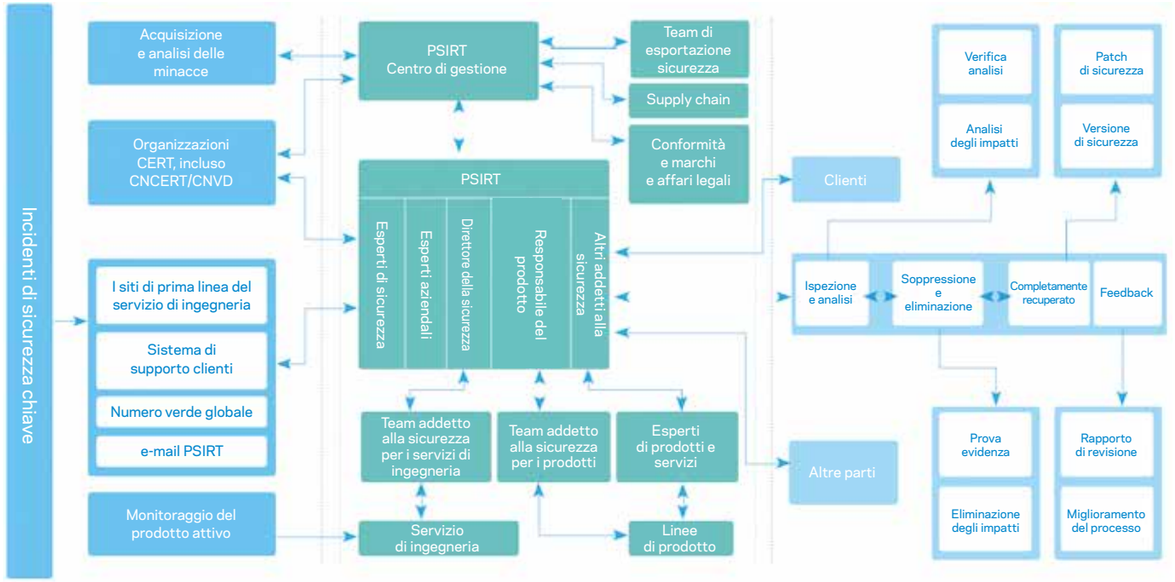
GESTIONE DEGLI INCIDENTI DI SICUREZZA

La sicurezza informatica può essere influenzata da molti fattori, ad esempio minacce, debolezze e vantaggi in termini di costi, quindi è difficile per noi eliminare tutti i rischi per la sicurezza.
Quando un rischio per la sicurezza diventa un incidente, oltre a fornire risposte tempestive ed efficaci, ZTE collabora anche con le parti interessate per sviluppare una soluzione in breve tempo al fine di ridurre qualsiasi impatto negativo causato dall'incidente di sicurezza. Insistendo sui principi dell'apertura e della trasparenza, ZTE assicura di esporre tempestivamente tutte le potenziali vulnerabilità del prodotto, incluse le soluzioni finali, ai clienti.

RISPOSTE AGLI INCIDENTI DI SICUREZZA INFORMATICA

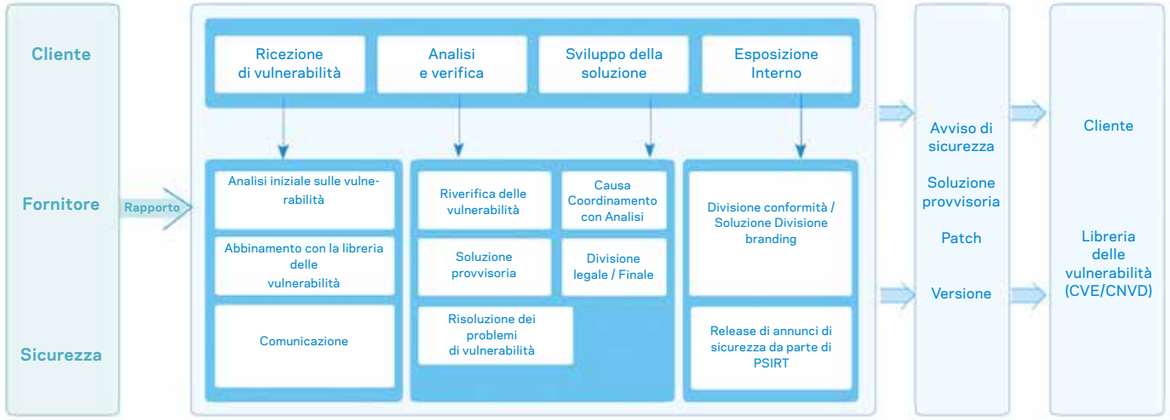
Il team PSIRT di ZTE è responsabile della ricezione, elaborazione e divulgazione delle vulnerabilità della sicurezza relative ai prodotti e alle soluzioni ZTE. Coordinandosi con clienti e le parti interessate, il team di PSIRT sviluppa rapidamente soluzioni. La creazione di un meccanismo chiave di risposta agli incidenti di sicurezza per gli incidenti di sicurezza (ad esempio, violazione dei dati) garantisce un coordinamento unificato, una riparazione rapida e un ripristino veloce del servizio.

Per gli incidenti di sicurezza, è già stato creato un meccanismo di gestione a ciclo chiuso che include misure di precauzione, ispezione, rettifica, ripristino e risposta dopo che il problema è stato risolto.
Una volta segnalato un incidente di sicurezza in base al risultato del monitoraggio giornaliero del prodotto, viene costituito immediatamente il team PSIRT composto da esperti di sicurezza, esperti aziendali, direttori della sicurezza prodotto, il referente del PSIRT e il chief security officer per analizzare gli incidenti e intraprendere le misure necessarie per controllarne lo sviluppo e assicurare che i servizi siano ripristinati.
È implementato un meccanismo di revisione dell'incidente per migliorare il processo di gestione e impedire che incidenti simili si verifichino nuovamente dopo l'incidente per garantire un controllo efficace.



GESTIONE DEL PROCESSO PER LE VULNERABILITÀ DELLA SICUREZZA

ZTE rafforza attivamente la propria cooperazione con le organizzazioni di sicurezza esterne. Per tutte le vulnerabilità identificate sia all'interno che all'esterno di ZTE, in base al principio di apertura e trasparenza, ZTE garantisce che vengano divulgate alle parti interessate. In qualità di membro del FIRST e della CVE Numbering Authority (CNA), ZTE si è dedicata alla pubblicazione delll'esposizione alle vulnerabilità di concerto con i clienti e le parti interessate in modo trasparente. Le vulnerabilità dei prodotti sono divulgate sui siti Web di ZTE e CVE. Per incoraggiare l'identificazione sia interna che esterna delle vulnerabilità del prodotto, ZTE ha formulato un programma di riconoscimento delle vulnerabilità.



Canali per la segnalazione di incidenti di sicurezza numero verde ed e-mail per supporto tecnico globale:
+86-755-26771900
support@zte.com.cn

Segnalazione, risposta e canali di comunicazione per incidenti di sicurezza
Email pubblica di PSIRT:
psirt@zte.com.cn

Canali per l'annuncio delle vulnerabilità di sicurezza
sito Web assistenza tecnica:
http://support.zte.com.cn

IL PROCESSO DI GESTIONE DELLE VULNERABILITÀ DI PSIRT INCLUDE LE SEGUENTI CINQUE FASI:

RICEZIONE DEI REPORT SULLE VULNERABILITÀ

Ricevere report su incidenti di sicurezza o vulnerabilità della sicurezza sia dall'interno che dall'esterno dell'azienda, inclusi i report di clienti, CERT esterni, White Hats, gruppi di ricerca sulla sicurezza e dipendenti interni. Per incoraggiare una divulgazione responsabile, al fornitore verrà fornito un periodo di tempo ragionevole per affrontare e risolvere i problemi prima della divulgazione.

ANALISI E VERIFICA

Il team di PSIRT avvia indagini e analisi non appena riceve un report sulle vulnerabilità. Conferma la vulnerabilità e quindi definisce rapidamente il livello di gravità. Durante la fase di analisi e verifica, il team PSIRT mantiene le comunicazioni con chi ha segnalato la vulnerabilità per garantire l'accuratezza e la tempestività del processo di analisi della vulnerabilità.

SVILUPPO DELLA SOLUZIONE

Il processo PSIRT e il processo di R&S sono strettamente correlati. Una volta confermata la vulnerabilità, i team di prodotto interessati devono attivare immediatamente il meccanismo di risposta per stabilire la causa, ispezionare prodotti correlati non identificati, sviluppare soluzioni di ripristino e testare l'efficacia delle soluzioni. Per le vulnerabilità già divulgate, lo sviluppo di una soluzione che includa una soluzione temporanea per affrontare tali vulnerabilità deve avere la priorità per garantire una risoluzione rapida.

DIVULGAZIONE

Nel processo di gestione di un incidente, il team PSIRT deve comunicare attivamente con chi segnala le vulnerabilità, i team di sviluppo prodotto e i clienti, per divulgare i problemi in modo trasparente e dettagliato, fornendo loro politiche e soluzioni per affrontare la vulnerabilità.

FEEDBACK

Una volta implementata una soluzione, la sua efficacia deve essere monitorata per garantire che non vengano rilevati ulteriori problemi, con l'applicazione di soluzioni iterative qualora fossero necessarie. Una "gestione a ciclo chiuso" della revisione degli incidenti consente a ZTE di migliorare continuamente la R&S dei prodotti e garantire che la sicurezza dei clienti sia mantenuta per l'intero ciclo di vita del prodotto, migliorando sia la qualità che la sicurezza.

GESTIONE DELLA CONTINUITÀ AZIENDALE

La Business Continuity Management (BCM) è un processo che esamina i vari fattori di rischio e la potenziale fragilità dell'azienda quando si trova di fronte a situazioni imprevedibili. ZTE ha stabilito un meccanismo di continuità aziendale e una serie di soluzioni basate sulla ISO 22301 per garantire che l'azienda abbia la capacità di continuare a erogare prodotti e servizi.

La BCM di ZTE copre sia i processi aziendali primari (che includono R&S, supply chain e servizi di ingegneria) sia i processi aziendali a supporto (che includono sistema IT, finanza, personale e conformità) nell'intero ciclo di vita del prodotto.

Le linee guida del processo BCM di ZTE sono: prendere precauzioni, ridurre i rischi, rispondere rapidamente e migliorare continuamente la capacità di BCM, in modo da proteggere gli interessi dei nostri dipendenti, clienti, azionisti, fornitori e altre parti interessate nella massima misura possibile

BCM e la gestione degli incidenti di sicurezza sono importanti salvaguardie per prodotti e servizi sicuri.
Il processo di risposta agli incidenti si concentra sulla capacità di ZTE di rispondere in modo rapido ed efficace, attenua gli impatti degli incidenti di sicurezza, garantisce il rapido ripristino delle attività e offre la migliore opportunità per testare l'implementazione del piano di continuità aziendale. BCM salvaguarda la gestione degli incidenti di sicurezza attivando il meccanismo di risposta agli incidenti e implementando il piano di continuità aziendale quando si verificano incidenti di sicurezza che riguardano l'azienda.

BCM IN R&S

I numerosi centri di R&S di ZTE possono fungere da supporto reciproco in circostanze di emergenza per garantire il rapido ripristino delle attività e la continuità.
Una serie di piani di gestione degli incidenti sono stati redatti per far fronte alle contingenze.
Per le richieste di brevetto da parte di terzi, vengono effettuate ispezioni periodiche sui brevetti da parte della R&S per evitare violazioni e licenze incrociate. Per affrontare il rischio di turnover del personale chiave, è stato sviluppato un meccanismo di fidelizzazione incentrato sul personale chiave. Per i principali rischi, sono impostati i KPI (indicatori chiave di prestazione) per un monitoraggio regolare al fine di evitare interruzioni dell'attività.

BCM IN SUPPLY CHAIN

La BCM della supply chain di ZTE viene implementata attraverso il meccanismo operativo Warroom, durante il quale vengono regolarmente adottate misure contro i rischi di approvvigionamento materiale identificati e vengono implementate misure di gestione delle crisi per far fronte alle emergenze.
ZTE ha elaborato una mappa dei rischi delle risorse di approvvigionamento per la gestione e il controllo dei rischi. Quando si verificano diversi tipi di emergenze, i fornitori, i materiali, i codici e i prodotti coinvolti e la gravità dell'impatto possono essere identificati rapidamente con l'aiuto della mappa dei rischi, consentendo una valutazione del rischio complessiva in modo tempestivo. Inoltre, la mappa dei rischi fornisce i dati necessari per supportare fortemente il monitoraggio quotidiano e la prevenzione dei rischi materiali.
Le basi produttive di ZTE a Shenzhen, Heyuan, Changsha e Nanjing possono fornire supporto reciproco tra di loro in termini di fabbriche, energia, materie prime e magazzini di prodotti finiti. Le basi produttive a Shenzhen, Nanjing e Heyuan possono fornire supporto reciproco tra di loro e anche alla base di Changsha in termini di business PCBA.

BCM IN SERVIZI DI INGEGNERIA

Sono state stabilite delle tattiche di continuità aziendale per i servizi di ingegneria, ovvero prevenzione e controllo pre-evento, risposta durante l'evento e ricostruzione post-evento, tutte e tre le aree che sono sistematicamente interconnesse. I piani di emergenza sono sviluppati per molteplici scenari aziendali basati sui disastri identificati e le esercitazioni in caso di disastro sono organizzate regolarmente per garantire la continua efficacia e la convalida di questi piani.
Il backup offsite per il disaster recovery viene realizzato tramite il nostro numero verde per proteggere i servizi del cliente da eventuali interruzioni. Quando un servizio estero locale si interrompe, una linea di assistenza globale in Cina può fornire servizi di supporto alternativi. In alcuni centri di assistenza clienti regionali oltreoceano, il servizio globale Inbound Contact viene applicato per fornire backup offsite ai numeri verdi per garantire che le chiamate in arrivo possano essere risolte instradando le chiamate verso la Cina in circostanze di emergenza.

BCM IN SISTEMI IT

ZTE ha creato un data center active-active a tre locali: il disaster recovery metropolitano active-active + offsite. Per i sistemi aziendali core, l'architettura active-active è applicata presso i data center aziendali (EDC) presso le sedi ZTE situate nel parco industriale Hi-Tech di Shenzhen e Xili di Shenzhen. Allo stesso tempo, all'EDC di Nanjing viene applicato un backup per il disaster recovery per sincronizzare i dati dell'ambiente di produzione con altri EDC, per far fronte a scenari di incidenti aggiuntivi. L'integrazione sistematica dei centri di disaster recovery active-active e offsite metropolitani migliora in modo efficace la continuità del sistema centrale.
La Divisione IT continua ad aggiornare le valutazioni dei rischi e il piano di analisi dell'impatto aziendale (BIA), mentre organizza le esercitazioni in diversi modi per fornire scenari di ripristino efficace del sistema core ogni anno. Riassumendo e analizzando i risultati delle esercitazioni, la Divisione reparto IT identifica eventuali lacune con la domanda effettiva e migliora continuamente. La gestione efficace della continuità dei sistemi IT offre un forte supporto e una protezione significativa per le attività costanti e continue del business dell'azienda.

VALUTAZIONE INDIPENDENTE DELLA SICUREZZA

Tra le tre linee di difesa della gestione del rischio, la valutazione indipendente della sicurezza è la seconda che valuta e supervisiona le pratiche di sicurezza della prima linea. La valutazione indipendente della sicurezza esamina a sicurezza informatica da molteplici punti di vista in base ai principi del controllo del rischio.
Questa seconda linea di difesa riduce i rischi per la sicurezza e implementa la gestione a circuito chiuso e ilmonitoraggio dei problemi identificati attraverso un meccanismo di supervisione e controllo, per realizzare il miglioramento continuo della governance della sicurezza informatica.

MECCANISMO DI CONTROLLO PER LA VALUTAZIONE INDIPENDENTE DELLA SICUREZZA

Durante il processo di governance della sicurezza informatica, è impostata la seconda linea di difesa per evitare il fallimento del meccanismo di gestione e controllo della sicurezza della prima linea di difesa e per identificare e risolvere i rischi in azienda. La valutazione e la supervisione della sicurezza e il diritto di veto della seconda linea di difesa sono applicati per ridurre i rischi che non possono essere identificati o implementati in modo insufficiente nelle pratiche di sicurezza della prima linea di difesa. ZTE ha sviluppato un meccanismo di controllo operativo per la valutazione indipendente della sicurezza al fine di garantire una verifica efficace. Il meccanismo di controllo operativo si basa su un sistema indipendente, automatizzato, completo e a circuito chiuso.
Indipendente: Le valutazioni della sicurezza della seconda linea di difesa sono completamente separate dalle attività nella prima linea di difesa e devono essere segnalate al Comitato di Cybersecurity (CSC).
La seconda linea di difesa ha discrezione sul processo e i risultati delle valutazioni, che non sono soggetti alle attività nella prima linea di difesa.

Indipendente

Le valutazioni della sicurezza della seconda linea di difesa sono completamente separate dalle attività nella prima linea di difesa e devono essere segnalate al Comitato di Cybersecurity (CSC).
La seconda linea di difesa ha discrezione sul processo e i risultati delle valutazioni, che non sono soggetti alle attività nella prima linea di difesa.

Completo

Le valutazioni della seconda linea di difesa monitorano l'intero processo di sicurezza, i meccanismi di gestione e controllo e i risultati finali della prima linea di difesa, concentrandosi sui processi e sui risultati della governance e caratterizzati da una supervisione a 360 gradi.

Automatizzato

La seconda linea di difesa può agire direttamente contro qualsiasi problema riscontrato nelle valutazioni. Ad esempio, se ci sono problemi che violano le red line della società, la seconda linea di difesa eserciterà i propri diritti di veto per conto di ZTE di sospendere immediatamente le attività commerciali incriminate delle unità coinvolte, tra cui l'interruzione della release di software e altre attività, mentre richiede alle unità coinvolte di sviluppare una risoluzione entro un determinato periodo

A circuito chiuso

Le valutazioni della seconda linea di difesa implementano la gestione a circuito chiuso e il monitoraggio dei problemi identificati, prestando attenzione alla risoluzione e ai risultati dell'eliminazione dei difetti. Solo i problemi che hanno superato la verifica possono essere definiti come risolti.

PROCESSO DI VALUTAZIONE INDIPENDENTE DELLA SICUREZZA

La verifica indipendente della sicurezza di ZTE segue un processo normativo che copre aree quali supply chain, R&S, consegna e risposta agli incidenti. Nella fase di pianificazione, vengono effettuati controlli a campione casuali sui prodotti di prima linea e sui progetti di servizi. Piani specifici sono sviluppati sulla base dei requisiti per la governance della sicurezza informatica. Nella fase di implementazione, le valutazioni vengono effettuate da due punti di vista.

Processo valutazione	Valuta l'efficacia dell'attuazione dei regolamenti e dei punti di controllo stabiliti dalle unità aziendali.
Processo valutazione	Valuta la sicurezza dei prodotti e dei sistemi e conduce analisi e valutazioni quali scansione delle vulnerabilità, audit dei codici di sicurezza e test di robustezza dei protocolli.

Durante la fase di riesame e reporting dei risultati, il riesame viene svolto sui risultati della valutazione e i risultati finali vengono comunicati al CSC. Inoltre, le vulnerabilità del prodotto rilevate verranno riportate nel sistema di gestione dei difetti. Sull'analisi verrà effettuato il monitoraggio a ciclo chiuso, per garantire il miglioramento e la verifica delle vulnerabilità. Nella fase di verifica, vengono eseguite ispezioni sulle migliorie apportate e un altro controllo a campione verrà effettuato in loco se necessario. La verifica deve essere effettuata sulla correzione dei difetti del prodotto, che verranno monitorati attraverso il sistema di gestione dei difetti fino alla risoluzione degli stessi.

METODI APPLICATI NELLA VALUTAZIONE INDIPENDENTE DELLA SICUREZZA

Più metodi vengono applicati nella valutazione indipendente della sicurezza per la valutazione e la verifica, ad esempio test per le funzioni delle linee di base di sicurezza, scansione di sicurezza e test di penetrazione. In questo modo, l'efficacia della governance della sicurezza dei prodotti di prima linea viene verificata da più punti di vista.

TEST PER LE FUNZIONI DELLE LINEE DI BASE DI SICUREZZA *Eseguito secondo le linee di base dei requisiti di sicurezza per verificare lo stato effettivo delle funzioni di sicurezza specificate nelle linee di base e l'efficacia di tali funzioni di sicurezza.*

SCANSIONE DI SICUREZZA *Vengono adottati strumenti di scansione accettati a livello industriale per verificare i risultati delle pratiche di sicurezza di prima linea, tra cui la scansione e il controllo della sicurezza del codice sorgente del prodotto e la scansione di sistemi operativi, database, servizi WEB e altri moduli di terze parti, a identificare le vulnerabilità dei sistemi e dei dispositivi.*

TEST DI PENETRAZIONE *Vengono effettuati test di attacchi simulati su prodotti e sistemi che, attraverso l'analisi degli scenari operativi reali dei prodotti e dei sistemi, analizzeranno i potenziali punti deboli, individueranno le vulnerabilità della sicurezza, eseguiranno l'analisi dei difetti e avanzeranno suggerimenti di miglioramento.*

AUDIT DI SICUREZZA

L'audit della sicurezza informatica fornisce ragionevoli garanzie alla direzione della società, i clienti e altre parti interessate circa l'implementazione efficace di politiche, regolamenti e processo di cybersecurity per soddisfare le esigenze dei clienti. Come terza linea di difesa per la governance della cybersecurity, audit di sicurezza per effettuare una valutazione indipendente sulla solidità, la razionalità e l'efficacia del sistema di sicurezza informatica della società, per spingere la società a rafforzare la costruzione del sistema di sicurezza informatica per implementare il sistema in modo rigoroso, assicurare i miglioramenti continui ed efficaci apportati al sistema e realizzare la supervisione e la gestione trasparente del sistema.

ZTE ha sempre avuto un atteggiamento aperto e trasparente nei confronti dei propri stakeholder chiave, ricevendo audit interni e audit esterni secondo lo statuto della società. Le relazioni di revisione sono presentate al Presidente per approvazione. Relazioni regolari sono presentate al Comitato di revisione o al Consiglio di amministrazione. I rischi riscontrati negli audit sono segnalati tempestivamente alla Direzione e al Consiglio di amministrazione.

Gli audit di sicurezza di ZTE vengono effettuati da più punti di vista, inclusi organizzazione e funzionamento, processi di gestione dei rischi, attività di controllo e supervisione interna, a copertura dei processi di sicurezza informatica end-to-end che includono la sicurezza R&S, la sicurezza della supply chain, la sicurezza della consegna, la risposta agli incidenti di sicurezza e la verifica indipendente della sicurezza.

Audit di Organizzazione e Operazione

Attenzione per gestione operativa integrata, competenze, reporting e meccanismi decisionali per importanti questioni di sicurezza informatica, ecc.

Audit di gestione dei rischi

Attenzione per individuazione, valutazione, gestione dei rischi di sicurezza informatica, istituzione e attuazione del meccanismo di segnalazione dei rischi, i piani di emergenza e le procedure e il meccanismo di rintracciabilità per gli incidenti di perdita di sicurezza.

Audit di efficacia

Le attività di controllo si concentrano sulla progettazione dei punti di controllo e la loro applicazione nel processo aziendale e l'effettiva attuazione dei punti di controllo.

A circuito chiuso

Attenzione per la supervisione giornaliera e meccanismo speciale di supervisione per la prima e la seconda linea di difesa, correzione dei problemi riscontrati e costruzione e attuazione del meccanismo di valutazione.

L'intero processo di revisione è orientato verso i rischi. ZTE rivede continuamente la robustezza e l'efficacia del sistema di cybersecurity dell'azienda per soddisfare i requisiti di sicurezza dei clienti e di altre parti interessate.

LABORATORI DI CYBERSECURITY LABS E COLLABORAZIONE ESTERNA

ZTE si confronta costantemente con gli standard di sicurezza e le migliori pratiche, collabora attivamente con le organizzazioni del settore e profonde sforzi per comunicare con i clienti e le altre parti interessate in modo aperto e trasparente e rafforzare la fiducia reciproca, per realizzare l'obiettivo comune di resistere alle minacce alla sicurezza informatica.

Il laboratorio per la sicurezza informatica è una delle misure adottate da ZTE per aumentare la trasparenza in tutto il mondo. Il laboratorio per la sicurezza informatica funzionerà in modalità "1+N", con il laboratorio principale in Cina e più punti di accesso remoto in Cina e in altri paesi. Con i vantaggi geografici determinati da una implementazione multinazionale, il laboratorio di sicurezza informatica fornirà servizi di valutazione della sicurezza esterni per clienti globali, autorità di regolamentazione e altre parti interessate aprendo il codice sorgente e i documenti del prodotto e fornendo servizi di valutazione della sicurezza multidimensionale.

Questi laboratori di sicurezza informatica saranno una piattaforma fisica per abilitare gli audit esterni di ZTE e la verifica indipendente, creando un ambiente aperto, trasparente e sicuro per la prima e la seconda linea di difesa affinché possano svolgere le loro funzioni.
Le tre funzioni preimpostate del laboratorio di sicurezza informatica sono:

- *Revisione e valutazione del codice sorgente dei prodotti ZTE in un ambiente sicuro.*

- *Fornitura dell'accesso a documenti tecnici importanti dei prodotti e dei servizi di ZTE.*

- *Abilitazione dei test di sicurezza sui prodotti e servizi di ZTE effettuati manualmente o con l'ausilio di strumenti automatici.*

Allo stesso tempo, ZTE sta cercando di costruire una partnership strategica con terze parti.
Le tecnologie e i servizi acquisiti da tale partnership saranno applicati nello sviluppo dei laboratori di sicurezza informatica, consentendo verifiche indipendenti di sicurezza, convalida e audit di sicurezza indipendenti.

GUARDARE AVANTI E AVANZARE INSIEME

ACRONIMO O SIMBOLO	NOME COMPELTO
3GPP	3RD GENERATION PARTNERSHIP PROJECT
5G	5TH GENERATION MOBILE COMMUNICATION
AEO	OPERATORE ECONOMICO AUTORIZZATO
BCM	GESTIONE DELLA CONTINUITÀ AZIENDALE
CC	CRITERI COMUNI
CERT	COMPUTER EMERGENCY RESPONSE TEAM
CNA	CVE NUMBERING AUTHORITIES
COP	COMUNITÀ DI PRATICA
CSA	CLOUD SECURITY ALLIANCE
CSC	COMITATO DI CYBERSECURITY
CVE	COMMON VULNERABILITIES & EXPOSURES (VULNERABILITÀ ED ESPOSIZIONI COMUNI)
CWE	COMMON WEAKNESS ENUMERATION
EDC	DATA CENTRE AZIENDALE
FIRST	FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS
GDPR	REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
HPPD	SVILUPPO DEL PRODOTTO AD ALTE PRESTAZIONI
IETF	TASK FORCE DI INGEGNERIA DI INTERNET
ISO	ORGANIZZAZIONE INTERNAZIONALE PER LA STANDARDIZZAZIONE
ITU	UNIONE INTERNAZIONALE DELLE TELECOMUNICAZIONI
PSIRT	TEAM DI RISPOSTA AGLI INCIDENTI DI SICUREZZA DEL PRODOTTO
SATRC	S: SISTEMA A: ASSET T: MINACCIA R: RISCHIO C: CONTROLLO
SSG	GROUPPO SICUREZZA SOFTWARE
STIG	GUIDA TECNICA DI IMPLEMENTAZIONE DELLA SICUREZZA

APPENDICE:
PRINCIPALI EVENTI CYBERSECURITY DI ZTE

2005

ZTE ha superato la certificazione ISO 27001 (Sistema di gestione della sicurezza delle informazioni), che copriva tutte le attività di ZTE. Nel 2014, ZTE è passata al livello successivo di certificazione ISO 27001: 2013. Nel 2017, ZTE ha ottenuto la certificazione ISO 27001: 2013 in più paesi, tra cui Cina, India, Stati Uniti, Germania, Paesi Bassi, Regno Unito, Francia e Italia. A marzo 2019, 14 filiali di nuova costituzione in Europa hanno superato la certificazione ISO 27001: 2013 in paesi quali Austria, Grecia, Spagna e Belgio.

ZTE ha assunto la posizione di Vicepresidente di ITU-T SG17. Da tempo ZTE è attivo in organizzazioni di standard internazionali come 3GPP, IETF, ITU-T e CSA e nei forum sulla sicurezza, svolgendo un ruolo centrale nella promozione del lavoro di standardizzazione nel campo della sicurezza.

2011

ZTE ha istituito il CSC che ha realizzato il programma di sicurezza informatica.

ZTE ha iniziato a certificare i prodotti di gestione della rete con i Common Criteria (CC). A partire dalla fine del 2018, 12 tipi di prodotti sono stati certificati con i CC, compresi i prodotti e i dispositivi tradizionali come la rete core, la rete di accesso, la trasmissione ottica, la gestione della rete, il router e il controller della stazione di base.

2013

ZTE ha istituito il laboratorio di sicurezza informatica, che era un ente di verifica indipendente della sicurezza all'interno dell'azienda che ha fornito una piattaforma integrata per valutazioni di sicurezza, sviluppo delle capacità di sicurezza, risposta agli incidenti di sicurezza, gestione delle conoscenze sulla sicurezza e scambi di tecnologia.

2014

ZTE ha emesso una serie di standard e regolamenti interni, compresi i requisiti generali e il quadro per le linee di base di sicurezza e protezione dei prodotti.

2015

ZTE è entrato a far parte del Forum of Incident Response and Security Teams (FIRST), con l'obiettivo di migliorare la capacità di risposta degli incidenti di sicurezza.

2017

ZTE ha superato la certificazione ISO 28000 (Sistema di gestione della sicurezza della Supply Chain), che copriva l'approvvigionamento, la produzione e la logistica di 26 tipi di prodotti di telecomunicazione (inclusi i dispositivi mobili). Nel 2017, ZTE ha ottenuto il certificato di operatore economico autorizzato (AEO) rilasciato dall'Organizzazione mondiale delle dogane.

ZTE ha istituito un sistema completo di sicurezza informatica che copre più aree, tra cui R&S, supply chain, servizi di ingegneria, risposta agli incidenti di sicurezza e verifica indipendente della sicurezza.

ZTE è diventata una delle CVE Numbering Authorities (CNA). Il CNA ha fornito canali per la divulgazione proattiva delle vulnerabilità della sicurezza.

2018

ZTE ha emesso le red line di sicurezza del prodotto.

ZTE ha apportato modifiche al CSC, i cui membri sono i vertici. L'organizzazione e l'implementazione dell'assicurazione di sicurezza hanno attraversato i livelli di gestione.

ZTE ha nominato Zhong Hong come Chief Security Officer della società.

ZTE ha iniziato a costituire un laboratorio di sicurezza informatica che verrà utilizzato nella modalità "1+N". Il laboratorio principale era in Cina e in Cina e in altri paesi sono stati istituiti più punti di accesso remoto. Nel 2019, ZTE stabilirà due laboratori di sicurezza informatica in Belgio e in Italia, dove verranno eseguiti audit del codice sorgente, revisione della progettazione della sicurezza e test di sicurezza.