Vil du opleve det bedste inden for netværkssikkerhed?

Lad **ZyXEL** være dit førstevalg

ZyXEL er den førende producent af integreret sikkerhedsudstyr til små og mellemstore virksomheder*

* Kilde: Infonetics Research, sendte enheder – Integrerede sikkerhedsenheder i segmentet $ 500 - $ 1.499, EMEA, januar 2013-juni 2014 .

#1

ZyXEL's produkter til netværkssikkerhed er ideelle for enhver organisation på op til 1.000 ansatte, og De tilbyder al den hjælp, der er brug for, for at sikre, at alle vigtige virksomhedsdata altid er beskyttet.

UTM – Klare fordele

- Betydelige besparelser på plads og omkostninger
- Hurtige installationer
- Reducerede administrationsudgifter
- Reducerede uddannelsesbehov
- Forenklet fejlfinding
- Optimal ydeevne
- Maksimal fleksibilitet

Vil du vide mere?

- www.zyxel.dk

Sikkerhedstrusler for små og mellemstore virksomheder – risikoen har aldrig været større

Hastigheden og mobiliteten i forbindelse med internetforbindelser har revolutioneret den måde, vi arbejder på i dag. Superhurtigt bredbånd, fiberforbindelse til kontoret og mobile smartenheder med 3G- og 4G-forbindelse har åbnet døren for produktivitet døgnet rundt, uovertruffen kundeservice samt fordelagtige nye indtægtsmuligheder.

Datalækage, dataødelæggelse, nedetid

Små og mellemstore virksomheder står over for de samme udfordringer i forbindelse med sikkerhed som de største multinationale selskaber. Risikoen er ligeså høj, men adgang til ledelsesressourcer og finansiering er mere begrænset. Den barske realiteter er, at din virksomhed dagligt står over for nye sikkerhedstrusler. Ondsindede apps, denial of service-angreb, spyware og malware skaber store udfordringer også for små og mellemstore virksomheder. Datalækage, dataødelæggelse og nedetid kan have en stor indvirkning på produktivitet og kundeservice og i sidste ende kan det skade virksomhedens omdømme og rentabilitet.

Vi leverer tryghed

Hos ZyXEL anerkender De behovet for solide og pålidelige sikkerhedsløsninger, uanset virksomhedens størrelse og budget. Deres mål at tilbyde en bred palette af sikkerhedsløsninger, som er prisbillige, fleksible og arbejdsbesparende, og som samtidig beskytter dine forretningsmæssige aktiver uden at belaste administrationen yderligere.

USG-produkter er vejen frem

Ved hjælp af en række fleksible indstillinger, der kan afpasses efter virksomhedens størrelse, kan deres UTM-firewalls give dig en enkel, strømlinet styring, maksimal netværkstilgængelighed samt alle de nyeste funktioner i næste generations firewalls, og dermed stoppe truslerne, før de får adgang til dit netværk.

Internetmisbrug: Truslen

Udbredelsen af spil, sociale netværk, chat og peer-to-peer-netværk er eksploderet, og det kan være et reelt produktivitetsproblem for små og mellemstore virksomheder. Desuden kan angreb via social manipulering og phishing få medarbejdere til at afsløre følsomme personlige eller virksomhedsrelaterede oplysninger, herunder brugernavne og adgangskoder.

Internetmisbrug: ZyXELs USG-løsning

Programintelligens: ZyXELs USG Desktop-serie kan identificere, kategorisere og kontrollere mere end 3.000 webprogrammer samt funktionsmåder inden for sociale netværk, spil, produktivitet og andet. Brugerne kan prioritere produktive programmer, regulere acceptable programmer samt blokere ikke-produktive programmer for at booste produktiviteten og forhindre misbrug af båndbredden.

Unified Threat Management – Næste generations firewalls

Deres UTM-enheder samler fra op til seks sikkerhedsenheder ved adgangspunkterne, hvilket giver mulighed for en enkel opsætning, styring og fejlfinding samt forbedret ydeevne. Enhederne giver den ultimative fleksibilitet, da virksomhederne kan vælge de bestemte moduler og funktioner, de har brug for, samt føje indstillinger til deres enhed efter behov. UTM-enheder er programfølsomme og kombinerer en firewall, antivirus, indbrudsregistrering og -forebyggelse samt VPN-egenskaber i en enkelt boks – alt sammen med en enkelt adminstrationskonsol. De beskytter ikke kun dit netværk mod eksterne trusler, men også mod internt misbrug af netværket. Det gør de ved at kontrollere adgangen til chat samt websteder for peer-to-peer-netværk og sociale netværk. Med UTM-enheder får du en enkel, universal løsning, der kan forhindre ondsindede angreb i at resultere i nedetid, datatyveri eller datatab, samtidig med at de beskytter netværksbrugernes produktivitet.

UTM, når det er bedst

Den helt nye ZyXEL USG-serie er bygget til at give en ultrahurtig ydeevne i forbindelse med firewall, VPN og UTM. De har inkluderet branchens bedste sikkerhedskomponenter og samlet dem i en enkel strømlinet administrationsgrænseflade. Med ZyXELs USG-serie i mellemklassen får små og mellemstore virksomheder høj netværkstilgængelighed, så de altid kan kommunikere online. Serien indeholder multi-WAN-justering af belastning og failover og en avanceret 3G USB-modem-supportliste til WAN-backup. Derudover understøtter serien IPSec-justering af belastning og failover, hvilket medfører øget robusthed for de mest missionkritiske VPN-installationer. ZyXELs USG-enheder inkluderer også en integreret WLAN-controller, hvilket giver mulighed for et skalerbart sikkert BYOD-netværk (Bring-Your-Own-Device) samt gæste- og møde-lokaleforbindelse.

Malware: Truslen

Malware er ofte skjult i spam-e-mails, på websteder eller i filer, der kan downloades. Virus, trojanske heste, skadelige apps, orme og mange andre typer af skadelig software, der er beregnet til tyveri, ødelæggelse af data samt nedetid, kan hurtigt spredes til et helt netværk og medføre katastrofale skader. Medarbejdere kan ved et uheld slippe malware løs ved at åbne eksekverbare filer i e-mails, installere uautoriseret software eller besøge skadelige websteder. De sikkerhedsrisici, der er forbundet med virksomhedens godkendte software, er også mål for malware, og skadelige tilfældige downloads kan blive installeret, når brugerne blot besøger uskyldigt udseende websider, der kan være kompromitteret. Derudover medfører stigningen i BYOD-netværk, at medarbejderne kan overføre malware til organisationen, når de opretter forbindelse til inficerede personlige enheder.

Malware: ZyXEL USG-løsningen

Bloker skadelige e-mails og skadeligt webindhold vha. klassens bedste malwarebeskyttelse samt indholdsfiltrering allerede i gatewayen. Dermed spredes det ikke til netværket.

Kaspersky anti-virus: Med Kaspersky SafeStream II gateway-antivirus får du omfattende beskyttelse i realtid mod malwaretrusler, før de spredes til netværket. Kasperskys gateway-antivirus kan identificere og blokere mere end 650.000 former for ved indgangen til netværket, og du får samtidig en lynhurtig streamet virusscanningsteknologi.

Anti-Spam: Med integration til et cloudbaseret system der samler informationer om spamkilder kan ZyXELs antispam levere præcis og øjeblikkelig beskyttelse mod spamudbrud ved på et enkelt minut at analysere data om afsenderens på baggrund af meget forskellige kilder. Systemt kan registrere spamudbrud i løbet af de første få minutter af udbruddet, uanset spamsprog eller format.

Datatabsbeskyttelse: ZyXELs system til indbrudsregistrering og forebyggelse anvender en DPI-teknologi (Deep packet inspection), som kan scanne flere lag og protokoller og dermed inspicere sikkerhedsrisici, der er usynlige for enkle port- og protokolbaserede firewalls. Med ZyXELs indbrudsregistrering og forebyggelse fjernes falske positiver vha. en database over malwaresignaturer, og funktionen yder effektiv beskyttelse mod indbrud via ukendte bagdøre.

Fjernadgang: Truslen

Fjernkontorer, mobilbrugere og medarbejdere med hjemmekontor har alle brug for og forventer den samme adgang til virksomhedens ressourcer som medarbejderne på hovedkontoret. Fjernadgangsforbindelser er dog det primære mål for hackere og datatyve, og beskadigede forbindelser kan derfor fungere som adgangspunkt for skadelig software til det registreret netværk.

Fjernadgang: ZyXELs USG-løsning

Robust VPN: ZyXELs USG'er understøtter IPSec-, L2TP over IPSec- og SSL-VPN med højt throughput for en række VPN-installationer af typen websted-til-klient og websted-til-websted. ZyXELs USG'er er forstærket med avanceret SHA-2-kryptering og er den sikreste VPN-forbindelse til virksomhedskommunikation.

SSL-inspektion: SLL-inspektion gør det muligt for ZyXEL USG at give omfattende sikkerhed politikgennemtvingelse. Dermed aktiveres programintelligensen samt id, indholdsfiltrering og antivirus i USG, og trafikken i krypterede SSL VPN-tunneler inspiceres og trusler, der sædvanligvis ikke opdages, blokeres.

Kontaktpersoner

Keld Hansen
Product Specialist
Zyxel
Telefon: +45 4355 9396
keld.hansen@also.com

Erik Gildberg
Product Manager
Zyxel
Telefon: +45 4355 8848
erik.gildberg@also.com