



Vijf zaken waar systeembeheerders wakker van liggen

Systeembeheerders hebben vaak nog een stoffig imago, maar ze zijn stiekem belangrijker dan menig werknemer denkt. Binnen veel organisaties wordt de druk op deze onmisbare pionnen steeds groter. Wij hebben de vijf grootste uitdagingen van systeembeheerders voor je op een rij gezet.

1. Hogere eisen aan performance en efficiency

Voor de directie van een organisatie is het van groot belang dat werknemers zo veel mogelijk efficiënt en productief werken. Dit vraagt om een hoge performance van de beschikbaar gestelde technologie. Het is de dagelijkse taak van systeembeheerders om ervoor te zorgen dat alles op technisch gebied op rolletjes loopt en supportaanvragen netjes worden afgehandeld. Wanneer je als systeembeheerder om hulp wordt gevraagd moet je altijd paraat staan. Op het moment dat medewerkers niet goed kunnen werken of een bedrijf met downtime te maken krijgt gaat dit ten koste van de productiviteit. Wil je dat medewerkers met een tevreden gevoel naar hun werk komen? Dan is het van groot belang dat de IT goed werkt. Maar het is misschien nog wel belangrijker dat werknemers technologie kunnen gebruiken waar zij zelf graag mee werken. Er zijn verschillende onderzoeken die uitwijzen dat het beschikbaar stellen van de juiste apparaten en systemen leidt tot groter werkplezier en, als gevolg, tot een hogere productiviteit. Breng dus in kaart welke groepen medewerkers je hebt door verschillende medewerkersprofielen (persona's) op te stellen. Door samen met de IT-manager een goed beeld te schetsen van de wensen van de medewerkers in jouw organisatie kun je de productiviteit van je medewerkers verhogen met inzet van de juiste IT.

2. Downtime is geen optie meer

IT is onmisbaar binnen het bedrijfsleven. Iedere werknemer heeft er op de een of andere manier mee te maken. De eisen worden daarnaast steeds hoger omdat eindgebruikers tijdens hun werk dezelfde kwaliteit eisen die ze inmiddels van de technologie in hun privéleven gewend zijn. Hier werkt vaak alles naar behoren en kunnen ze apparatuur zo instellen dat het volledig naar eigen zin is ingericht. Op hun werkplek verwachten ze eigenlijk hetzelfde. Downtime is een van de grootste frustraties van de eindgebruiker en moet dus altijd voorkomen worden. Door deze ontwikkeling ligt er meer druk op systeembeheerders en ontstaan veel verschillende problemen, ook problemen waarvoor op dat moment enige vorm van kennis ontbreekt.

3. Kennis is key!

De cloud, hyperconverged infrastructures, cybercriminaliteit: zomaar wat thema's die zich de laatste jaren enorm hebben ontwikkeld. Als systeembeheerder ben je nooit uitgeleerd en ontwikkelingen volgen elkaar in rap tempo op. Dit is leuk, maar kan ook als uitdagend worden ervaren. Want dit vraagt om een hoop zelfstudie, vaak naast je dagelijkse werkzaamheden. Toch is het belangrijk om up-to-date te blijven. Organisaties die onvoldoende kennis in huis hebben zijn genooddaakt te werken met slecht functionerende systemen, waardoor werknemers minder goed hun werk kunnen doen. Zorg er dus voor dat je goed getraind bent en geef tijd aan wanneer je merkt dat je kennis achteropraakt.

4. Een wildgroei aan devices en applicaties

Werknemers hebben tegenwoordig gemiddeld drie tot vijf devices op zak. Dit brengt niet alleen de nodige beheerissues met zich mee, maar geeft ook connectiviteitsuitdagingen. Het liefst zijn we op al deze devices verbonden met het draadloze netwerk, maar hoe meer apparaten verbonden zijn met het draadloze netwerk, hoe groter de securityrisico's. Daarnaast zorgt de toename van het aantal devices per werknemer ook voor meer Shadow IT. Dit is de software en hardware binnen jouw organisatie die niet officieel zijn goedgekeurd. Het gebruik van bedrijfsapplicaties kun je namelijk goed beveiligen, maar applicaties die werknemers zelf installeren, bijvoorbeeld omdat ze hier in hun privéleven ook gewend aan zijn, leveren wat uitdagingen. Denk bijvoorbeeld aan applicaties als Dropbox of Google Drive. Iedereen gebruikt dit soort opslagsystemen, maar het is niet veilig genoeg om bedrijfsgevoelige informatie in op te slaan. Deze uitdagingen moeten worden afgevangen in een gedegen ICT-beleid. Stem goed af welke applicaties wel en niet zijn toegestaan en hoe je omgaat met de verschillende devices binnen je bedrijfsnetwerk.

5. Security, security, security

Wist je dat meer dan 95% van alle beveiligingsfouten veroorzaakt wordt door menselijk handelen? De één klikt op een phishingmail of verliest een USB-stick, de ander vergeet een back-up te maken of deelt onbewust informatie met ongeautoriseerde personen. Eindgebruikers zijn daarom zelf de essentiële schakel binnen informatiebeveiliging. Technische en organisatorische maatregelen zijn noodzakelijk om systemen up-to-date te houden en te zorgen dat de ICT goed beveiligd is. Maar het creëren van awareness bij medewerkers is minstens zo belangrijk. Systeembeheerders moeten ervoor zorgen dat de eindgebruikers fungeren als de human firewall van jouw organisatie. Maar hoe doe je dit? De eerste stap is bewustwording. Wist je bijvoorbeeld dat frauduleuze partijen veel verschillende manieren inzetten om achter gevoelige (bedrijf)informatie te komen? Daarnaast vormt het actief herkennen van veiligheidsrisico's, incidenten en kwetsbaarheden een belangrijke stap. Zo zorg je ervoor dat je jezelf en jouw organisatie beschermt. Jij en de eindgebruiker maken het verschil!

