SECURITY AUDIT

Questo documento presenta i risultati anonimi del controllo di sicurezza eseguito tramite la soluzione Safetica. L'analisi è stata effettuata su 83 postazioni di lavoro nel periodo di tempo dal 1 º marzo 2019 al 19 marzo, 2019. I dati si riferiscono all'orario di lavoro dell'azienda (dalle 7:00 alle 16:00).

safetica®

Sommario

SCOPO DELL'AUDIT

L'audit di sicurezza si concentra sui file sensibili nell'ambiente aziendale, sui file che escono dall'azienda e come i dipendenti utilizzano le risorse aziendali.

L'audit si basa sui file monitorati e sull'attività degli utenti sui computer su cui è stato implementato Safetica. I problemi di sicurezza e le precauzioni consigliate vengono valutati in base ai file che avete classificato in Safetica come sensibili, ai metodi sicuri che avete scelto per il trasferimento di contenuti sensibili e a quali siano le attività rischiose svolte dai dipendenti.

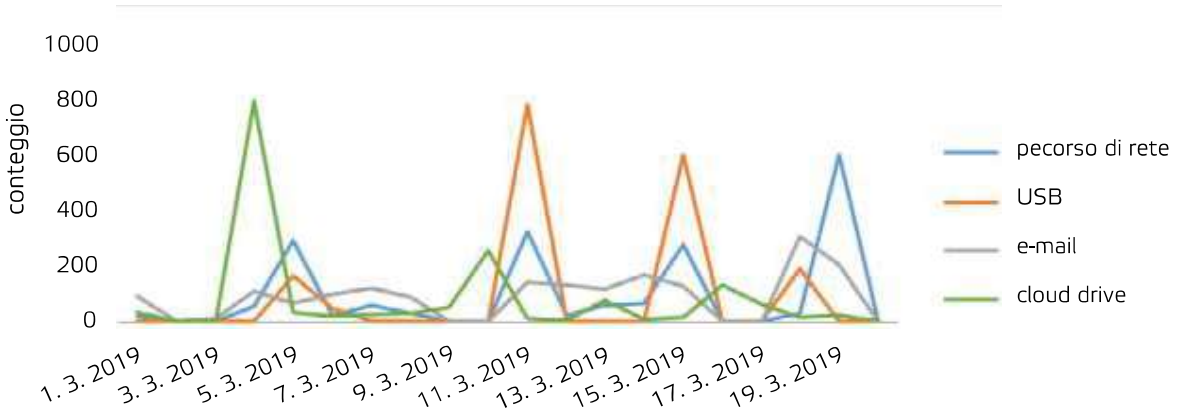
Dati monitorati:

- **301 GB** di dati
- **91.599** operazioni sui file
- **33.032** file
- **4.240** file in uscita

Ambienti monitorati:

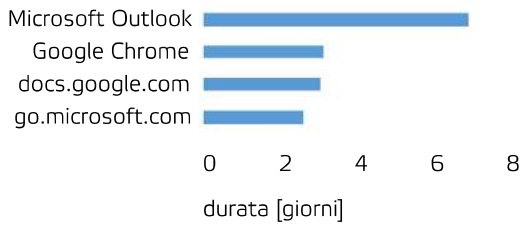
- **321** account utenti
- **83** computers con Safetica
- **223** computer in totale
- **42** amministratori Safetica

Quando sono stati inviati i file?



Che categorie di dati avevano i file?

Quali sono state le attività più comuni?



In caso di incidente di sicurezza, sarai avvisato da allarmi istantanei.

Se si verifica un problema di sicurezza, una risposta rapida è importante per ridurre al minimo gli impatti negativi. Avvisi istantanei al persone responsabili ti aiuteranno a capire rapidamente dove è sorto il problema.

Hai impostato rapporti regolari sullo stato di sicurezza dell'azienda.

L'ispezione regolare dello stato di sicurezza dell'azienda è una parte vitale della strategia di sicurezza complessiva.

Hai identificato i dati sensibili dell'azienda che devono essere protetti.

Senza sapere quali siano i dati aziendali sensibili, non è possibile applicare criteri di sicurezza per prevenire fughe di dati.

Raccomandazioni:

- Verificare regolarmente che gli allarmi impostati siano aggiornati e siano indirizzati al responsabile.
- Impostare rapporti regolari per le aree selezionate.
- Verificare regolarmente che i rapporti impostati siano aggiornati e siano indirizzati al responsabile.
- Controllare regolarmente con quali dati stanno lavorando i dipendenti e identificare i file sensibili.
- Classificare i file con dati sensibili su base regolare.

FILE TRASFERITI TRAMITE USB O ALTRI DISPOSITIVI ESTERNI

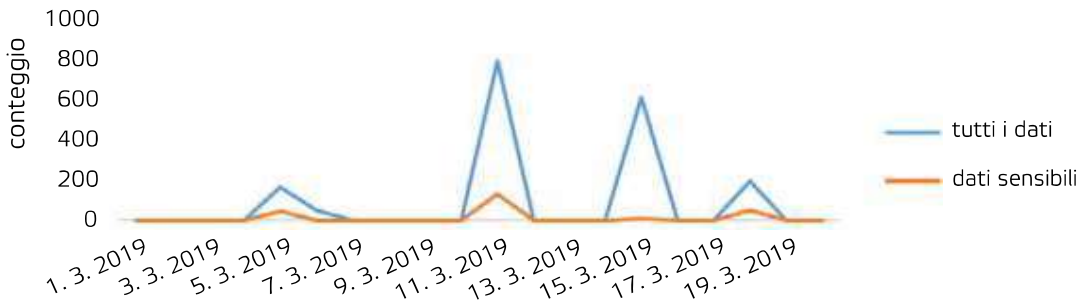
Caricare un gran numero di file sensibili su un flash drive USB è il modo più facile per perdere il controllo sui propri dati. Se l'USB è perso o rubato, dati critici possono cadere in mani non autorizzate.

223 file sensibili su un totale di 1793 file sono stati trasferiti tramite USB o altri dispositivi esterni. esterni. Le vostre policy di sicurezza non erano restrittive.

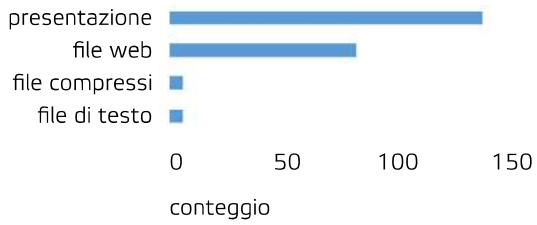
Trasferire dati al di fuori dell'azienda tramite un dispositivo USB è un rischio significativo. Accertarsi che i dispositivi USB siano sicuri è una misura necessaria.

15 file sensibili di un totale di 16 file sono stati trasferiti tramite USB o altri dispositivi esterni. Questi file hanno seguito le vostre policy di sicurezza.

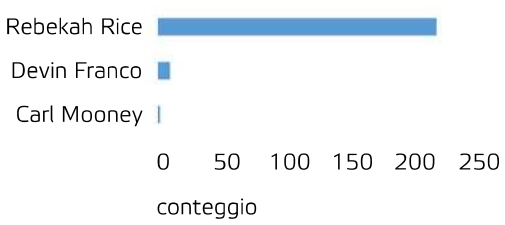
Quando sono stati inviati i file?



Quali categorie di dati sensibili sono state trasferite?



Chi ha inviato più dati sensibili?



Raccomandazioni

- Definire quali dispositivi USB ed esterni sono affidabili.

FILES TRASFERITI TRAMITE E-MAIL

Gli allegati e-mail sono uno dei modi più facili per l'esfiltrazione di dati sensibili. Nella maggior parte dei casi, il danno all'azienda è accidentale più che intenzionale – mandare all'errato destinatario o inviare

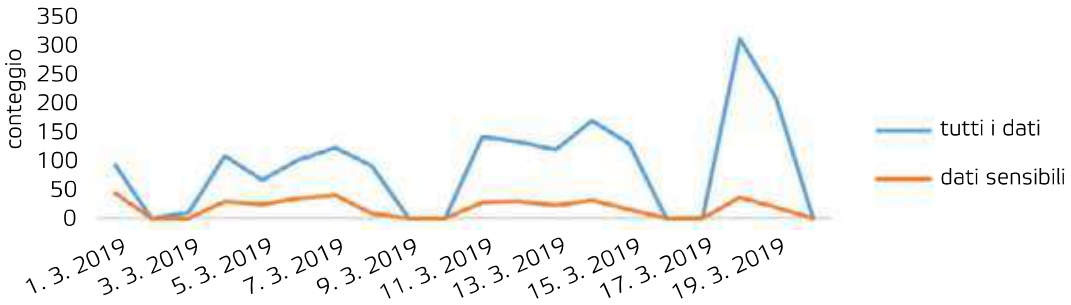
3 file sensibili di un totale di 124 file sono stati trasferiti via e-mail. Questi file non sono stati controllati da nessuna policy di sicurezza.

E-mail con dati sensibili dovrebbero essere inviati solamente a destinatari affidabili che devono lavorare con i dati.

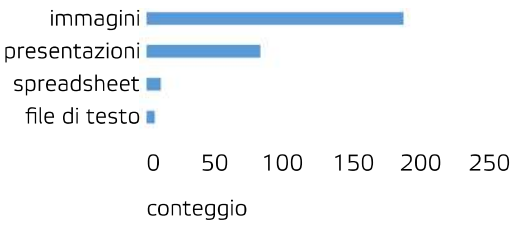
121 file sensibili di un totale di 121 file sono stati trasferiti via e-mail. Le vostre policy di sicurezza non erano restrittive.

241 file sensibili di un totale di 1557 file sono stati trasferiti via e-mail. Questi file hanno seguito le vostre policy di sicurezza.

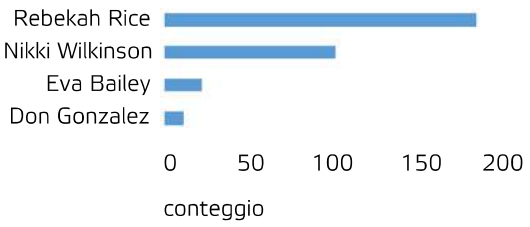
Quando sono stati inviati i file?



Quali categorie di dati sensibili sono state trasferite?



Chi ha inviato più dati sensibili?



Raccomandazioni:

- Definire gli ambienti aziendali affidabili per le e-mail.
- Revisionare regolarmente i domini affidabili per le e-mail.
- Verificare regolarmente dove sono inviate le e-mail.
- Verificare se gli allegati e-mail devono essere catalogati come dati sensibili.

FILES TRASFERITI TRAMITE WEBMAIL

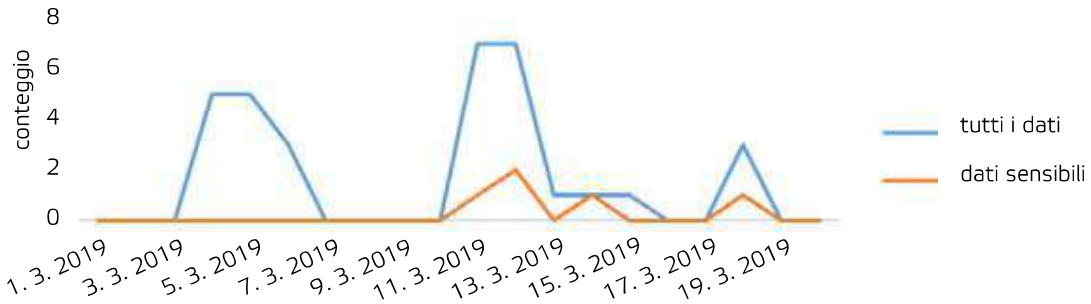
I servizi di posta elettronica Web sono popolari per la comunicazione e l'invio di file sensibili. Allo stesso tempo, però, questa forma di comunicazione è un altro canale di rischio che deve essere protetto da potenziali fughe di dati.

⚠ 3 file sensibili su un totale di 31 file sono stati trasferiti tramite webmail. Le vostre policy di sicurezza non erano restrittive.

Utilizzare i servizi webmail per inviare contenuti sensibili è un problema di sicurezza perché non è possibile controllare i destinatari nell'endpoint.

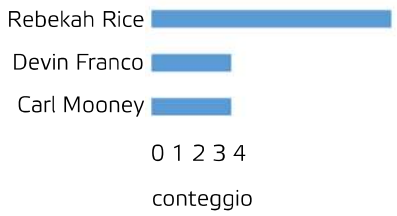
✓ 2 file sensibili di un totale di 2 file sono stati trasferiti tramite webmail. Questi file hanno seguito le vostre policy di sicurezza.

Quando sono stati inviati i file?



Dove sono stati inviati i file sensibili?

Chi ha inviato più dati sensibili?



ℹ Raccomandazioni:

- Determinare quali servizi webmail sono affidabili

FILE AZIENDALI CARICATI SUL WEB

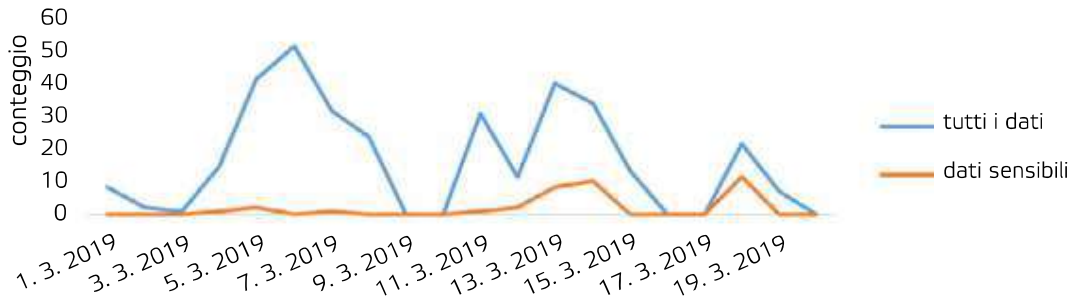
Caricare (upload) files sul web è un sistema popolare tra gli utenti per condividere file di grandi dimensioni che non possono essere inviati come allegati e-mail. E' perciò importante definire regole per inviare file attraverso questo canale.

⚠ 11 file sensibili di un totale di 298 file sono stati trasferiti via web upload. Le vostre policy di sicurezza non erano restrittive.

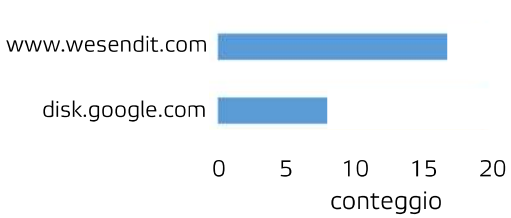
File aziendali che sono caricati su siti pubblici possono essere istantaneamente scaricati da sconosciuti e in questo modo voi ne perdete il controllo.

✓ 25 file sensibili di un totale di 25 file sono stati trasferiti via web upload. Questi file hanno seguito le vostre policy di sicurezza.

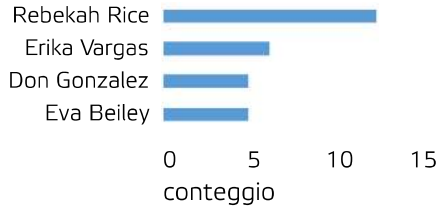
Quando sono stati inviati i file?



Dove sono stati inviati i file sensibili?



Chi ha inviato più dati sensibili?



ⓘ Raccomandazioni:

- Definire siti web affidabili per l'ambiente aziendale.

FILES TRASFERITI TRAMITE APP DI INSTANT MESSAGING

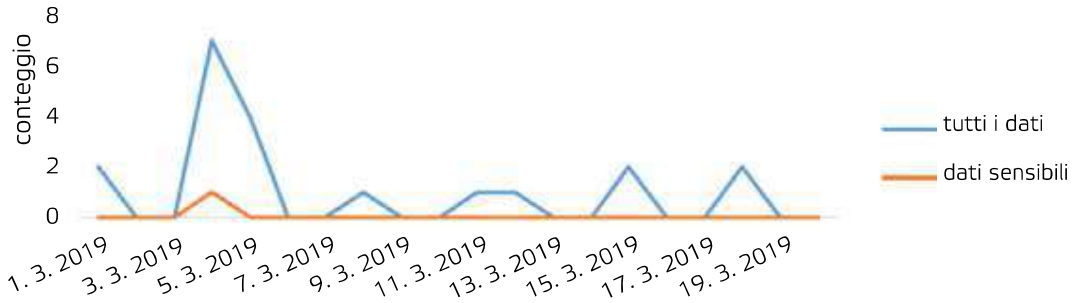
Le applicazioni di messaggistica istantanea sono uno strumento di comunicazione per lavorare con colleghi e partner in tutto il mondo. Sebbene l'invio di file sia limitato a una ristretta cerchia di destinatari, la messaggistica istantanea rappresenta una minaccia per le aziende che non monitorano e controllano l'uso di queste applicazioni.

18 file sono stati trasferiti via instant messaging. Le vostre policy di sicurezza non erano restrittive.

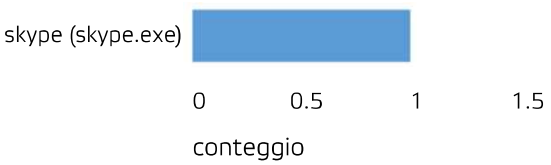
Inviare files aziendali senza nessuna restrizione tramite applicazioni di instant messaging mette a rischio i dati aziendali.

1 file sensibile di un totale di 2 file è stato trasferito via instant messaging. Questo file ha seguito le vostre policy di sicurezza.

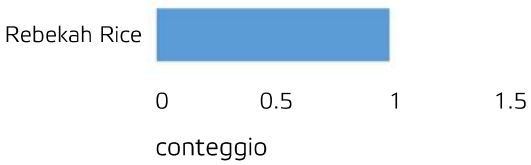
Quando sono stati inviati i file?



Dove sono stati inviati i file sensibili?



Chi ha inviato più dati sensibili?



Raccomandazioni:

- Definire le applicazioni di instant messaging affidabili per l'ambiente di lavoro.

FILES TRASFERITI TRAMITE SERVIZI DI CLOUD STORAGE

File aziendali possono esfiltrare quando vengano trasferiti a storage in cloud personale con insufficienti settaggi di sicurezza.

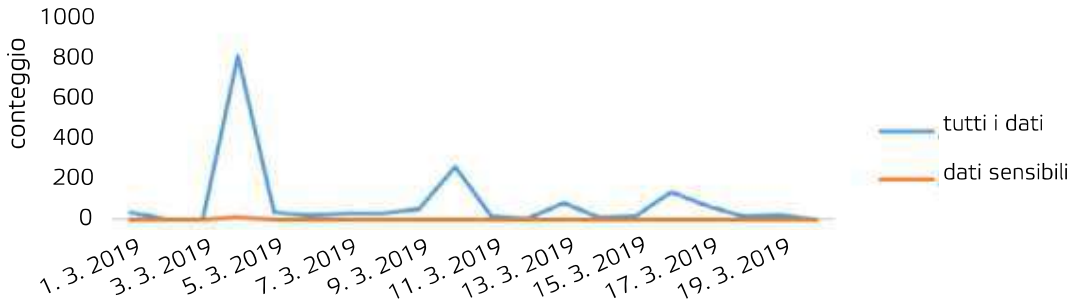
18 file sono stati trasferiti tramite servizi cloud storage. Questi file non sono stati controllati da nessuna policy di sicurezza.

Utilizzare servizi coud storage personali o non autorizzati presenta rischi di sicurezza per file aziendali sensibili.

10 file sensibili di un totale di 673 file sono stati trasferiti tramite un servizio di cloud storage. Le vostre policy di storage non erano restrittive.

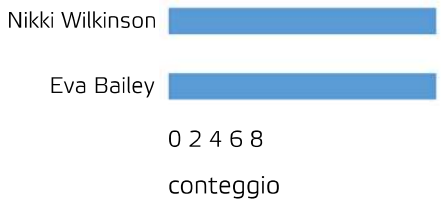
2 file sensibili di un totale di 1072 file sono stati trasferiti tramite un servizio di cloud storage. Quesi file hanno seguito le vostre policy di sicurezza.

Quando sono stati inviati i file?



Quali categorie di dati sensibili sono state trasferite?

Chi ha inviato più dati sensibili?



Raccomandazioni:

- Definire un ambiente di lavoro affidabile per i servizi di cloud storage.

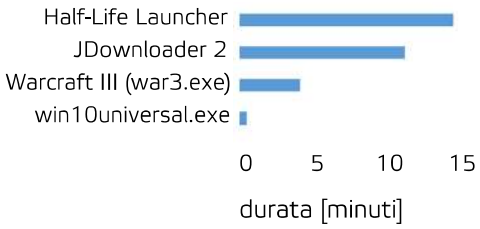
ANALISI DI COME SONO USATE LE APPLICAZIONI

Capire quali applicazioni usano gli utenti aiuta le aziende a scoprire dove ci sono rischi di sicurezza, come vengono utilizzate le costose licenze software, e come la produttività può essere migliorata.

Avete limitato l'utilizzo di applicazioni rischiose che non possono essere usate dagli utenti.

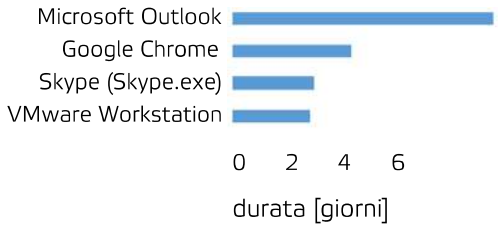
Regole ben definite riguardo l'utilizzo di applicazioni aumenta la sicurezza dell'azienda.

Quali sono state le attività rischiose più comuni?

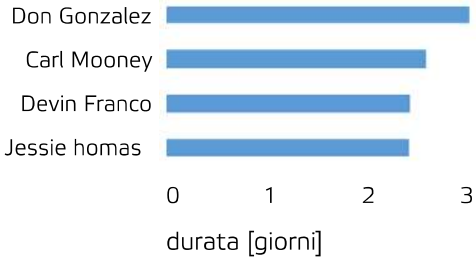


Come hanno utilizzato il loro tempo di lavoro gli utenti?

Quali sono state le attività più comuni?



Chi è il più attivo?



Raccommandazioni:

- Catalogare periodicamente le applicazioni monitorate.

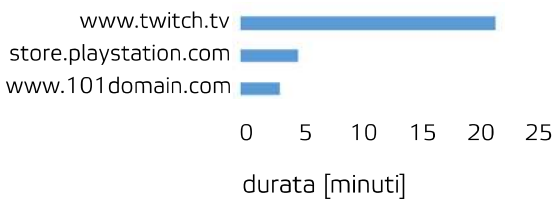
ANALISI DELL'USO DEL WEB

Capire quali siti visitano gli utenti aiuta le aziende a scoprire dove ci sono rischi di sicurezza o dove la produttività può essere migliorata.

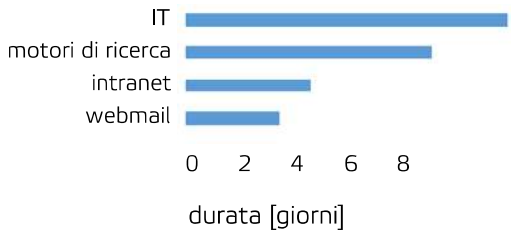
Avete limitato siti web rischiosi che non possono essere visitati dagli utenti.

Regole ben definite riguardo la navigazione web aumenta la sicurezza dell'azienda.

Quali sono state le attività rischiose più comuni?

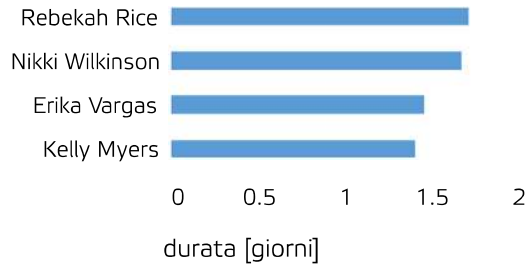


Come hanno utilizzato il loro tempo di lavoro gli utenti?



Quali sono state le attività più comuni?

Chi è il più attivo?



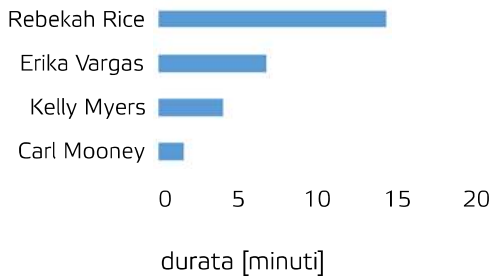
Raccomandazioni:

- Catalogare regolarmente i siti web monitorati.

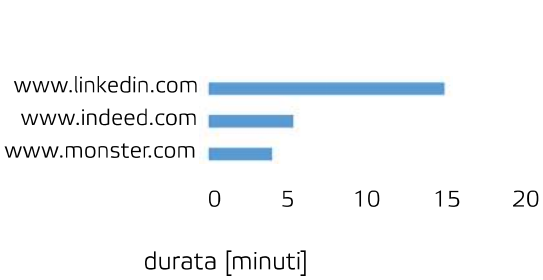
ANALISI DELL'USO DI SITI PER LA RICERCA DI LAVORO

Dipendenti che scelgono di lasciare l'azienda costituiscono un significativo rischio alla sicurezza. Se accedono a un nuovo lavoro, con un concorrente ad esempio, e portano con sé importanti documenti, il danno per la vostra azienda può essere sostanziale.

Quali sono state le attività rischiose più comuni?



Come hanno utilizzato il loro tempo di lavoro gli utenti?

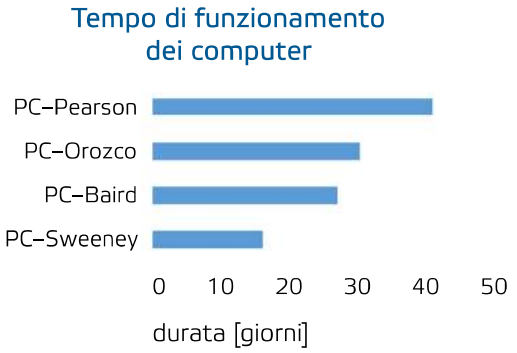


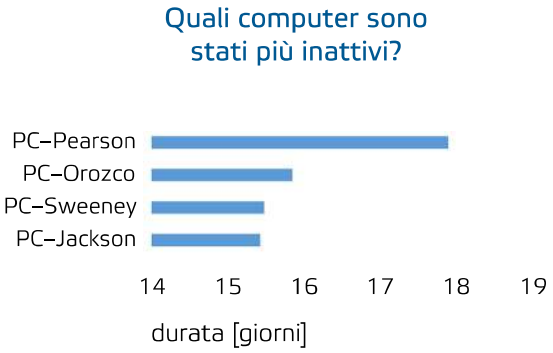
Raccomandazioni:

- Catalogare regolarmente i siti web di ricerca lavoro monitorati.

USO DELLE RISORSE IT – COMPUTER

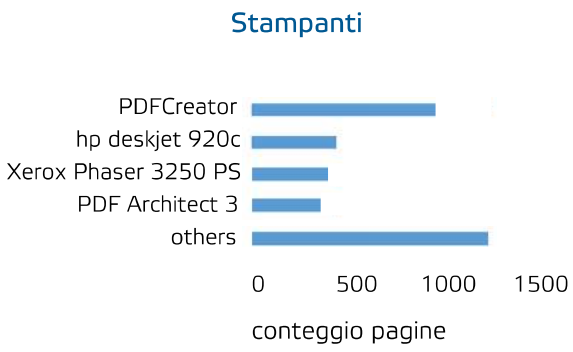
L'uso efficiente dei computer aziendali è importante per capire dove è possibile realizzare risparmi.





USO DELLE RISORSE IT – STAMPANTI

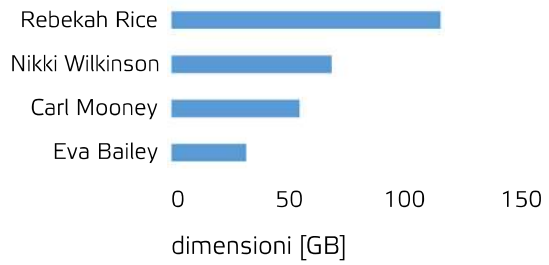
Un report dell'uso delle stampanti vi aiuterà a capire se i documenti stampati presentano rischi o costi non necessari per l'azienda.



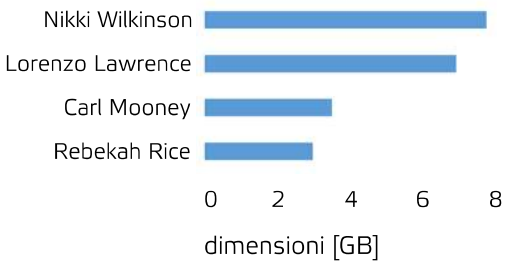
USO DELLE RISORSE IT – TRAFFICO DI RETE

Sovraccaricare o inviare grandi quantitativi di dati attraverso la rete può costituire un rischio per la sicurezza dell'azienda o ridurre la produttività del lavoro degli altri dipendenti.

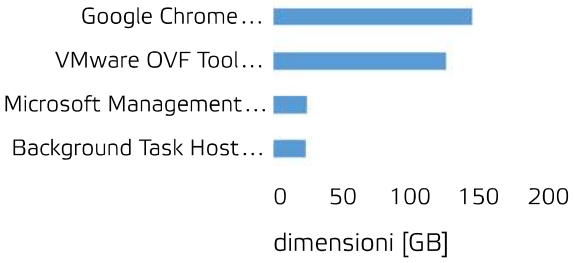
Download degli utenti



Upload degli utenti



Download delle applicazioni



Upload delle applicazioni